KYLINSOFT
麒麟软件

银河麒麟高级服务器操作系统 V10 SP3 2403

版本发布说明

麒麟软件有限公司

2024 年 03 月

1. 版本概述

此次发布的是银河麒麟高级服务器操作系统 V10 的第四个版本。本说明列举了银河麒麟高级服务器操作系统从 V10 SP3 版本到 V10 SP3 2403 版本的主要更新内容。

2. 版本信息

类型	版本信息
产品名称	银河麒麟高级服务器操作系统 V10
ISO 名称	Kylin-Server-V10-SP3-General-Release-2403-X86_64 Kylin-Server-V10-SP3-General-Release-2403-ARM64 Kylin-Server-V10-SP3-General-Release-2403-LoongArch64.iso
发布格式	ISO、虚拟机镜像、容器镜像
版本查询方式	终端：输入 cat/etc/.kyinfo 查询 图形界面:所有程序->关于银河麒麟

3. 技术参数

类型	参数信息
支持架构	ARM、X86、龙芯
支持处理器型号	● 飞腾：FT-2000+/64、腾云 S2500、腾云 S5000C ● 鲲鹏：920、920 V200 ● 海光：海光 1 号、海光 2 号、海光 C86-3G、海光 C86-4G ● 兆芯：开胜 ZX-C+、开胜 KH-20000、开胜 KH-30000、开胜 KH-40000 系列 ● 龙芯：龙芯 3B5000、龙芯 3C5000L、龙芯 3C5000、龙芯 3D5000 ● Intel/AMD 等服务器平台
支持固件类型	BIOS/UEFI
内核版本	4.19.90
Glibc 版本	2.28-98
GCC 版本	7.3.0-2020033101

Java 版本	java-11-openjdk-11.0.22.7、java-1.8.0-openjdk-1.8.0.402
开发语言支持	C/C++、Java、Go、Python、Php、Perl、ruby 等
桌面环境	UKUI 2.0
中文支持	GB18030-2022
虚拟化	KVM/qemu/libvirt
授权方式	在线、离线、KMS 机制
补丁更新	每周
客户群体	全行业用户
配套文档	银河麒麟高级服务器操作系统 V10 安装手册 V4.0 银河麒麟高级服务器操作系统 V10 系统管理员手册 V4.0 银河麒麟高级服务器操作系统 V10 安全中心用户手册 V4.0 银河麒麟高级服务器操作系统 V10 文件保护箱用户手册 V4.0 银河麒麟高级服务器操作系统 V10 日志查看器用户手册 V4.0 银河麒麟高级服务器操作系统 V10 加固手册 V4.0 银河麒麟高级服务器操作系统 V10 安全三级加固手册 V4.0

4. 主要更新

- 新增支持飞腾 S5000C 芯片及其新特性，包括网络亲和性、PCIe/DDR PMU 驱动、Arm64 架构 ACPI/APEI 特性等；
- 新增支持鲲鹏 920+ 芯片及其新特性，包括 PTT 驱动、SPI/SFC 驱动、ll_cache_miss_rd 和 ll_cache_rd 通用事件等；
- 新增海光 C86-4G 芯片及其新特性，包括虚拟化和安全特性增强等；
- 新增兆芯 40000 新增 SM2 加密算法驱动支持，以及兆芯平台 PMU 增强、MWAIT C-state 等新特性支持；
- 新增龙芯 LoongArch64 架构新增 3D5000 芯片及其新特性，包括 BTF 属性、ETMEM 和 SRIOV 等；
- 新增 vrcraid、sssraid 阵列卡、SSSNIC/3s9xx 网卡、沐创网卡驱动 rnpgbe、7

09 显卡驱动、JM9200 景嘉微显卡、楠菲网卡 PS1600 等驱动支持；

- 内核特性增强，主要在 I/O 存储和网络、容器和虚拟化、进程调度、ebpf、RAS 和安全特性等方面
- 新增系统诊断工具，如 io 问题排查 iodump、网络诊断 nettrace、网络延迟探测 pingtrace；
- 新增智能运维助手，通过命令行方式提供日志收集、系统体检、系统监控功能；
- 新增一键式性能调优工具，收集服务器的全量性能数据，形成可视化报告，并直观展示异常指标及调优建议；
- 虚拟机热迁移功能增强，迁移数据支持国密；
- 提供容器在离线混合功能 rubik；
- 支持安全启动、支持国密和机密计算、可信软件栈支持 TPM2.0 和 TCM1.2，合入安全套件 SDK 接口。

5. 附录 1 更新内容

5.1. 功能变动与性能提升

5.1.1. 平台硬件适配

- 飞腾 S5000C 网络亲和性支持
- 飞腾 S5000C PCIe/DDR PMU 驱动支持；
- 新增 Arm64 架构 ACPI/APEI 特性支持

- 新增飞腾 CEU 算法驱动支持
- 新增飞腾 E2000 BMC 内置显示驱动支持
- Optee 新增飞腾设备树描述信息支持
- 新增飞腾 S2500 RAS 基础功能支持
- 新增 X100 相关 SOC 外设驱动
- ARM64 架构新增 AMU 扩展属性支持
- 新增 Phytium DDR/C2C/PCIE PMU 支持

- 鲲鹏 920+ 新增 HISI PTT 驱动支持
- 鲲鹏 920+ HISI SPI/SFC 驱动支持
- 鲲鹏 920+ HISI 架构新增 ll_cache_miss_rd 和 ll_cache_rd 通用事件支持
- 鲲鹏 920+ HISI ras 功能增强
- LoongArch64 架构新增 BTF 属性支持
- LoongArch64 架构新增 ETMEM 支持
- LoongArch64 架构内核提供新的 vmlinuz.efi 镜像文件
- LoongArch64 架构 kdump 功能增强
- 新增 LoongArch64 的内核 page dump 支持
- LoongArch64 架构 ls2k500sfb 内置显示驱动增强
- LoongArch64 架构新增 SRIOV 支持
- LoongArch64 架构使能 rubik 支持

- 新增 LoongArch64 平台 ls2k500sfb BMC 支持
- 新增 LoongArch64/X86 架构 Inspur BMC 显示驱动支持
- 龙芯 ls2k500 内置显示驱动增强
- ETMEM 驱动新增 LoongArch64 架构支持

- 更新兆芯 GMI SM3/SM4 内置驱动
- 兆芯 40000 新增 SM2 加密算法驱动支持，添加对 ZXPAUSE 指令的支持
- 兆芯平台新增 SM3/SM4 硬件算法支持
- 兆芯平台增强 PMU 支持
- 兆芯架构新增 MWAIT C-state 支持
- 新增 Hygon 4 号支持
- Hygon 平台 虚拟化增强

- 新增 vrcraid 阵列卡驱动支持
- 新增 sssraid 阵列卡驱动支持
- 新增 ARM64 架构的 SM3/SM4 驱动支持
- 新增 SSSNIC/3s9xx 网卡支持
- 新增沐创网卡驱动 rnpgbe 支持
- 新增 TCM2.0 支持
- 新增 709 显卡驱动 ljmcore 2.2.4.1 版本
- 新增 JM9200 景嘉微显卡驱动

- 新增楠菲以太网卡 PS1600 驱动支持
- 新增 Intel QAT 驱动
- 新增 Mucse RNP/RNPVF/RNPM 网卡驱动支持
- ARM64 新增 JM9200 显卡驱动支持

- 更新 lpfc 驱动到 14.2.0.7
- 更新浪潮显示驱动到 0.2 版本
- Megeraid 硬件 RAID 驱动更新到 07.719.03.00-rc1 版本
- 硬件 RAID 驱动 smartpqi 更新至 2.1.20-035 版本
- 内核更新 qla2xxx 驱动至 10.02.06.200-k 版本
- 网讯网卡驱动 ngbe 更新至 1.2.5 版本
- 网讯网卡驱动 ngbevf 更新至 1.2.1 版本
- 网讯网卡驱动 txgbe 更新至 1.3.4 版本
- 光润通网卡驱动升级至 1.23.815 版本
- 更新 IGC 网卡驱动
- 更新 MUCSE 网卡驱动 rnpvf 到 0.2.0 版本
- 更新 MUCSE 网卡驱动 rnpm 到 0.2.0 版本

5.2. 内核

5.2.1. I/O 存储和网络

- 多路径支持 Historical Service Time (HST) 和 I/O Affinity 路径选择器

- X86 EXT4 文件系统新增加密支持
- 新增硬件 RAID + NVMe 优化组件
- IO 栈去掉 block 层单队列支持，所有设备都转为多队列支持
- 新增 PCIe 5.0 特性支持
- overlayfs 新增 userxattr 属性支持
- 新增 BFQ IO 调度优先级策略 QOS 支持
- 在 Bonding 的 balance-alb/balance-tlb 模式下，新增 IPv6 ns/na 支持
- 新增支持 ipv6 DNR 双转发功能
- 新增 Nvme-Over-Tcp 支持
- NVMe 新增 host-auth 和 target-auth 支持
- 新增 net.ipv4.sysctl_tcp_tw_timeout 支持
- X86 架构使能 CONFIG_GENERIC_PHY=y
- 调整 Nvme 相关的设备驱动由 y 到 m
- 新增 ACPI HMAT 支持

5.2.2. 容器和虚拟化

- 新增 VirtIO 1.1 版本特性支持
- memcg 新增 memory.events 和 memory.events.local 接口
- 新增 vcpu stall detector 检查器
- 新增 cgroup freezer controller 特性支持

- 内核新增混部 SMT 驱离防止优先级反转特性支持
- 新增 CPU 调度负载均衡混合部署特性功能
- 新增 MemCG 异步水位线混合部署特性功能
- Arm/arm64 新增 PTP_KVM 支持
- 开放 sched qos 在线离线混部的自低优先级调整到高优先级的限制
- 使能 CONFIG_VHOST_SCSI=m
- 在 ARM64/X86 放开 cpu 混部负载均衡使能开关

5.2.3. 进程调度

- 新增 IO 亲和调度器支持
- ARM64 新增 CLUSTER 调度域
- 调整 ARM64 架构的默认抢占策略为 PREEMPT_VOLUNTARY
- 关闭 SCHED_AUTOGROUP

5.2.4. ebpf 增强

- eBPF 新增 bpf_for_each_map_elem helper 接口支持
- eBPF 新增 ringbuf 支持
- eBPF skb_verdict 新增 SK_PASS 特性支持
- eBPF TRACING 模式中支持 bpf_get_socket_cookie helpers
- eBPF 新增 eBPF BTF_KIND_FLOAT 支持
- eBPF 新增 bpf_redirect_peer 接口，满足 cilium 支持需求

- eBPF 新增 bpf_bpf_redirect_neigh 接口，满足 cilium 支持需求
- eBPF 新增 bpf_ktime_get_boot_ns 接口
- eBPF 新增 skb 丢包 Reson 类型支持

5.2.5. RAS 增强

- PCIe AER 错误上报机制增强
- HNS3 网卡驱动新增 RAS 故障上报支持
- Kunpeng memory RAS 特性功能增强
- 修复 rasdaemon 报告的 diskerror_eventstore 问题

5.2.6. 安全增强

- KYSEC 新增显示 HOOK 权限控制节点
- KYSEC 在网络管控中使用 blacklist 进行过滤
- KYSEC 新增设备管控相关的支持
- 新增 SELinux/ngac hook 接口
- 新增 SELinux ngac hook 支持
- IPsec XFRM 新增 SM3/SM4 算法支持
- 使能 KIC 安全框架支持

5.2.7. 性能调优

- 优化硬件 **RAID + NVMe** 存储性能

- 优化 MLX5/I40E 在 S5000c 接收性能
- 优化网讯网卡驱动 txgbe IPv4 转发性能
- 优化 txgbe 驱动在飞腾 S2500 10GB 性能
- 软 raid10 锁优化，性能提升
- 优化 sched 调度器 vdso 获取时间逻辑
- 优化 ARM64 系统调用接口性能
- 优化飞腾 2000+ 和鲲鹏 920 在某些情况下 UnixBench 分值
- 优化 Loongarch 架构 lmbench 性能
- 优化 tcp skb 释放逻辑，加速高速网卡极限性能
- 优化 i40e 的 TCP_RR/TCP_CRR 等性能
- 调整 tk_core 结构内存布局，优化鲲鹏 920 的 UnixBench 性能
- 调整低端内存布局，优化鲲鹏 920 UnixBench shell 执行效率
- 优化 seccomp 特定 smb 屏障，加速 UnixBench syscall 执行效率
- 优化 HugePage 大页初始化时，内存占用过大

5.2.8. 其他特性

- page_owner 新增 timestamp 和 pid 以及进程名称的支持
- perf 新增 ARMv8.3-SPE 支持
- 新增内核启动参数 hostname=xxx 来设置默认的 hostname
- 新增 RCU stall diagnosis information 特性支持
- 新增 UKFEF 统一内核故障框架支持

- 内核新增 available_filter_functions_addrs 接口，用于过滤跟踪函数以及提供函数地址
- 内核新增 ARM64 高性能特性 LSE 支持
- X86 架构新增 CONFIG_CPU_FREQ_GOV_SCHEDUTIL 调频支持
- Arm64 新增 CONFIG_FB_LS2K500 模块支持
- 新增 USB/raw-gadget 支持
- 新增 KT0206 音频卡驱动支持
- 新增 CONFIG_EFI_TEST=m
- LoongArch64 架构新增打包 cpupower 工具
- ARM64 4k 内核 CONFIG_STACKPROTECTOR_STRONG 编译增强
- 内核提供 kernel-doc 包
- 内核关闭 Logo 显示
- 不再为 ARM 平台提供 ls2k500sfb 显示驱动支持
- 关闭默认的 kfence

5.3. 基础组件

5.3.1. glibc：系统基础库

- 在 init_cacheinfo 中增加对兆芯的虚拟机检测支持；
- 增加对 GB18030-2022 新国标编码的支持
- 添加兆芯补丁，提升 memcpy 等接口的性能；

5.3.2. systemd：用户空间管理

- 移除可执行文件的 rpath/runpath 属性值、提升安全；
- 添加一些内存 overflow 溢出检查
- 使每个标签以 nul 终止，防范 dns_label_unescapetriggers 缓冲区溢出
- 添加出错后正常 return 返回动作
- udev 日志增加 udev rules 文件的 mode 属性打印
- udevadm 中启用 usec_add()
- 优化 install_context_apply()的错误码
- udevadm trigger 模块优化返回码的处理
- 增加 pstore 中 dmesg 信息存储状态检查
- 优化 udev 规则属性文件中的换行符处理
- 优化 udev 退出时对 workers 的等待处理
- 优化 systemd 对 daemon 程序的 trigger 逻辑条件
- udevadm trigger 中增加忽略 EROFS
- 优化 sd-event 模块中其他线程对默认事件循环不执行
- time-util 模块增加支持用户空间的 time_t 是 64 位但是内核不是的系统
- time-util 模块对 EOVERFLOW 错误处理中增加 32 位长的处理
- 优化 udev 规则文件的匹配逻辑中的文件权限设定
- 优化 udev 网络对 bit rate 的存储、全部由改为 uint_64_t
- 为 systemd-networkd.service 增加 AF_ALG、满足 Khash 需求
- udevadm info 增加更多的错误信息展示

- udevd 避免杀死运行中的 worker 进程
- 优化 Exec*指令中的“+”前缀处理逻辑忽略 PrivateTmp 等文件系统方面的选项
- journalctl 命令新增功能参数--facility=kern；
- journal 执行失败增加打印日志；
- 切换 su 到普通用户，执行 busctl 命令时增加 Interactive authentication 回显；
- 函数接口改名优化：函数 is_dir_fd()和 is_dir()变为内联函数，统一调用 is_dir_full()函数；
- 函数 config_parse_si_size 变更改为 config_parse_si_uint64；

5.3.3. xorg-x11-server：图形服务

- 增加 multi-gl sietium driver 支持；
- 增加芯动科技风华显卡支持；
- 增加支持凌久 GP201 显卡驱动。

5.3.4. audit：系统审计服务

在 auditd 停止时释放异步刷新锁

audit 设备管控需求合入通用,添加程序黑名单类型

添加 kysec_ppro 和 kysec_netctl 日志类型

5.3.5. cryptsetup：存储加密

- 优化: 在没有对齐最小页大小的情况下不再报告最优 IO 大小。
- 添加了对新的 no_read/write_wrokqueue dm-crypt 选项的支持。
- 增加了对 dm-verity 设备的 panic_on_corruption 选项的支持。
- 支持用于在线 LUKS2 重新加密的 --master-key-file 选项。
- 将一些 libcryptsetup 函数的返回错误码调整为 EEXIST,以便调用者可以分辨出该调用失败是因为某个并行进程已激活设备。
- TrueCrypt/VeraCrypt 兼容模式现在支持激活具有更大的扇区的设备。
- 当我们使用 --offset 指定的大小创建 LUKS2 header 时，如果参数指定的大小大于 LUKS2 的 header 的大小，则不创建。
- integritysetup 支持新的 dm-integrity HMAC 重新计算选项。
- integritysetup 在 dump 命令中显示重新计算扇区。
- 如果哈希区域为空，则不处理哈希图像。
- veritysetup 将 verity 哈希算法以小写形式存储在超级块中，否则，内核可能会拒绝激活设备。
- 在尝试打开 NTFS 设备时显示更好的错误。
- 添加对启动密钥保护的 VMK 的支持。
- 如果不支持调整设备大小，则打印可见错误。
- 挂起错误的非 LUKS 设备时添加错误消息。
- 重新表述丢失锁定目录警告，并将其移至调试级别。
- 允许具有 cipher_null 的设备恢复 LUKS。
- 当数据密码为空时，不要在密钥环中上传密钥。
- 重新加密 cipher_null 设备时切换到默认密码。
- 在重新加密之前替换可能的伪密文。

- cryptsetup 备份标头可用于激活 TCRYPT 设备，使用--header 选项指定标头。
- 为加密后端添加 Blake2b 和 Blake2s 哈希支持。
- 支持外部 LUKS 令牌插件。
- 提供一个实验 SSH 令牌。
- 添加 cryptsetup --token-type 参数， 将令牌类型限制为参数值。
- 支持使用 PIN 进行基于令牌的激活。
- 通过基于令牌的激活尊重密钥槽优先级。
- 默认 LUKS2 PBKDF 现在为 Argon2id。
- 将 Argon2 基准测试的最低内存成本提高到 64MiB。
- 自动检测 LUKS2 格式的最佳加密扇区大小。
- 默认情况下使用 VeraCrypt 选项，并添加--disable-veracrypt 选项。
- 支持--hash 和--cipher 来限制 TCRYPT 类型的打开时间。
- integritysetup 添加完整性重新计算重置标志。
- cryptsetup 在 LUKS2 的 luksChangeKey 中保留 keyslot 编号。
- 添加关闭 --deferred 和 --cancel-deferred 选项。
- 重写命令行选项解析以避免 libpopt 参数内存泄漏。
- 添加 --test-args 选项。
- veritysetup: 添加 --root-hash-file 选项。
- libcryptsetup C API 扩展（有关详细信息，请参阅 libcryptsetup.h）
- 将令牌分配给非活动密钥槽时打印错误消息。
- 不允许对具有数据偏移量的设备进行 LUKS2 解密。

5.3.6. dnsmasq：域名服务

- 添加--dynamic-host 选项：将 A 和 AAAA 记录添加到与指定接口位于同一子网的 DNS 解析中。
- 添加--bogus-nxdomain 选项：将包含指定地址或子网的恢复转换为“无此类域”的回复。
- 添加--ignore-address 选项：忽略对包含指定地址或子网的 A 或 AAAA 记录的查询请求。
- 根据--dns-forward-max 配置的值缩放 DNS 随机端口池的大小。

5.3.7. e2fsprogs：EXT 文件系统工具

- libext2fs 批量调用 ext2fs_zero_blocks2()，加快 mkfs.ext3 的运行速度。

5.3.8. gcc：系统编译器

- 对 int128 位的使用判断条件进行了逻辑调整，不需要在 gcc 的 configure 阶段通过 glibc 的相关宏定义的值来判断是否可以使用 int128 位的长类型，而是在运行时，通过 sizeof 的值来判断。更符合交叉编译的使用场景的逻辑。
- 新增支持 AutoBolt 特性， BOLT(Binary Optimization and Layout Tool)是链接后优化(post-link optimizer)，使用基于采样的 profile 信息，甚至可以对已经进行过 FDO(feedback-driven optimization) 和 LTO(link-time optimization)之后的二进制，再次提升其运行性能，所以这是一个可

作为补充的优化手段。

- 优化 kernel 的 pgo 优化过程，使用此选项编译出的内核，在二次编译的时候会使用相关数据对性能进行提升，patch 中的内容是 gcc 侧的修改，kernel 也有需要配合修改的部分。
- 对于不需要寄存器保存的栈帧也进行初始化，在 chain 中进行管理。
- 新增 bytes_below_hard_fp 来保存栈低和栈顶之间的距离。
- 新增 bytes_above_locals 来保存局部区域和栈顶之间的距离。
- 增加对 cpu 核心 tsv110 的支持，此核心支持 v8_4A 指令集扩展
- 增加 tsv110 流水线调度
- 中端优化部分，对冷热点优化的判断进行了重构
- 对循环优化措施的中间表示层-tree 进行优化。
- 去掉 bolt 特性在自动反馈优化部分的内容。不影响-fbolt-use 和-fbolt-target 的使用。

5.3.9. java-11-openjdk：java 语言

- 新增-h 命令参数。
- TLS, 1.2 的默认 Diffie-Hellman 密钥大小从 1024 位增加到 2048 位。这是为了增强加密强度。如果需要，可以通过设置 jdk.tls.ephemeralDHKeySize 系统属性回退到 1024 位。
- SunJSSE 提供程序现默认使用服务器端的密码套件偏好，而不是客户端指定的偏好。可以通过 SSLParameters.setUseCipherSuitesOrder(false)恢复旧行为。

- JDK 现在接受 PKCS#1 格式的 RSA 密钥。这意味着 RSA 密钥可以在更多格式下使用。
- 在 JAAS 的 ChoiceCallback 和 ConfirmationCallback 类中，现在会克隆传入构造函数或返回的数组，提高了安全性。
- 从 cacerts 密钥库中移除了 SECOM Trust System 的 RootCA1 根证书。
- 向 cacerts 信任库中添加了 Certigna Root CA 证书。
- 如果无法加载 java.security 文件，将抛出 InternalError 错误，而不是使用旧的安全属性集。
- 为支持 GB18030-2022 标准，JDK 11 增加了五个额外的字符支持。
- 支持 GB18030-2022 标准，与 Unicode 11.0 同步。可以设置系统属性 jdk.charset.GB18030 为 2000 使用旧版本字符集。
- 引入了系统属性 jdk.jar.maxSignatureFileSize 来配置 JAR 文件验证期间签名相关文件的最大字节数。
- 加强了对 ZIP 文件中 Zip64 字段的检查。如果导致可信 ZIP 文件失败，可以通过设置系统属性 jdk.util.zip.disableZip64ExtraFieldValidation 为 true 来禁用这些检查。
- javadoc 工具增强，允许包含与标准 Doclet 生成的文件的许可相关的法律文件。
- 改进了 Swing 平台的支持。现在，嵌入在 Swing HTML 组件中的 HTML 对象标签仅在设置了新的系统属性 swing.html.object 为 true 时才会渲染。
- 从默认启用的 TLS 协议中移除了 SSLv2Hello 和 SSLv3。要启用 SSLv3，需要使用特定的系统属性或编程方式设置。
- 向 cacerts 信任库中添加了 Certigna(Dhimyotis) Root CA 证书。

- 默认情况下，禁用了在 BMP 图像中加载链接的 ICC 配置文件。可以通过设置系统属性 sun.imageio.bmp.enabledLinkedProfiles 为 true 来重新启用。
- 默认情况下，禁用了 com.sun.media.sound.JARSoundbankReader 实现从 URL 下载 JAR 声音库的行为。
- 更新了 LoginModule 实现，以检查和处理空值。
- 默认情况下，禁用了使用 SHA-1 算法签名的 JARs。
- 更新了 PKCS#12 密钥库中默认的 MAC 算法，基于 SHA-256，比基于 SHA-1 的旧算法更强。
- 使用 JDK Flight Recorder (JFR)可以监控对象的反序列化。
- 在 Kerberos 中弃用并默认禁用了 des3-hmac-sha1 和 rc4-hmac 加密类型。
- 更新了 java.util.Vector，以在反序列化期间正确报告 ClassNotFoundException。
- 为 Java GSS/Kerberos 通过 HttpsURLConnection 添加了 HTTPS 通道绑定支持。
- 修改了 DeflaterOutputStream.close()和 GZIPOutputStream.finish()方法，在传播异常之前关闭相关的默认 JDK 压缩器。
- 对 java.io.File 进行了更严格的文件路径有效性检查。
- SunPKCS11 提供程序增强以支持 ChaCha20-Poly1305 密码和 ChaCha20 密钥生成器。
- GC.heap_dump 诊断命令新增 gz 选项，用于启用堆转储的 gzip 压缩。
- 引入了两个新的系统属性，用于禁用客户端和服务器端的 TLS 扩展。
- SunPKCS11 提供程序新增配置属性，以更好地控制原生资源的使用。

- ZIP 文件系统提供程序现在会拒绝包含带有"."或".."的条目的现有 ZIP 文件。
- 从 cacerts 密钥库中移除了 Google 的 GlobalSign Root 证书。
- 更新了 IANA 时区数据库至 2021c 版本。

5.3.10. java-1.8.0-openjdk：java 语言

- Cgroup v2 支持: OpenJDK 8 现在能够在 Linux 容器环境中准确识别和处理 cgroup v2，
- Java 应用可以更有效地管理和使用容器分配的资源，例如 CPU 和内存限制。
- 文件系统改进: 加强了对 Windows NTFS 交替数据流（ADS）的支持。
- GB18030-2022 标准支持:更新了对中国国家标准 GB18030-2022 编码的支持。
- TLS 1.3 支持: OpenJDK 8 现在默认启用 TLS 1.3 协议，提供更强的安全性和性能。
- 移除了一些不再安全的根证书，并添加了新的根证书，以维护 Java 应用和库与外部系统的安全通信。
- 安全算法和协议改进: 对 Kerberos 认证协议和 PKCS#12 密钥和证书管理标准的实现进行了加强，提高了安全性和可靠性。
- 对 Swing 和 AWT 库进行了性能优化，改善了对高 DPI 显示器的支持和图形渲染性能。
- 加强了 Swing 组件中 HTML 内容的安全处理，增强了对潜在的恶意代码的防护。同时提高了图像处理库（如 libpng）的安全性和稳定性。
- 对 HotSpot 虚拟机进行了一系列的性能优化和稳定性修复，包括改进垃圾回收机制，提高了 Java 应用的运行效率和响应性。

- 修复了 HotSpot 虚拟机中发现的多个安全漏洞，增强了 Java 运行时环境的安全性。
- 增强了 JVM 的诊断和调试功能，使开发者和运维人员能够更有效地监控和调试 Java 应用。
- 对 CORBA（一种用于分布式应用的中间件技术）的序列化处理进行了安全性增强。
- 更新了图像处理相关的库，例如 libpng，以提供更好的性能和安全性。

5.3.11. linux-firmware：驱动固件

- 系统增加集成 Intel E810XXVDA2 25G PCIE 型号网卡驱动
- 核外增加支持芯启源 Agilio GX 系列网卡驱动

5.3.12. lm_sensors：传感器工具

- 针对虚拟机场景，新增-n 选项，在虚拟机中启动服务时使用/usr/bin/sensors -s -n 来支持在虚拟机中启动服务即使没有检测到硬件传感器也不报错。

5.3.13. libabigail：ABI 兼容性

- 强化了类型规范化，包括即时规范化和避免过早规范化枚举。
- 引入了新的命名类型定义使用，支持了 DWARF 不完整类类型。
- 允许对联合类型进行克隆数据成员。
- 把函数类型变化视为局部变化，并添加了相关的调试工具。
- 通过改进 Bloom 过滤器位的使用和其他速度提升。
- 优化了 `change_kind` 枚举值的一致使用和局部变化的表示。

- 处理每个翻译单元和每个语料库的类型映射，以及去重处理。
- abidiff:在报告版本不匹配时包含 ABI XML 版本。
- kmidiff:为比较内核树添加了 CTF（Compact C Type Format）调试信息的支持。
- 添加了使用 CTF 信息执行 abipkgdiff 的回归测试。
- ctf-reader 完善了对 CTF 调试信息的支持。
- ctf-reader 增加了支持在外部路径查找调试信息的功能。
- 支持了多个--headers-dir 选项以执行 abidiff 和 abidw。
- 改进了内部表示的调试功能。
- IR: 支持复制 Union 的数据成员。
- IR: 避免取消一个已经"确认"的传播的规范化类型。
- DWARF 读取器：接受位于 .dynamic 段内的 SHT_PROGBITS 节。
- DWARF 读取器：使用 size_t 来表示 DWARF 表达式的长度。
- 改善了类型作用域在类型规范化时的更新。
- 提升了 Linux Kernel 二进制文件的类型比较优化。
- 处理了大型二进制文件时的自检失败问题。
- 增强了内部表示的调试功能，包括为枚举类型显示支持。
- 添加了针对 abidiff 的 --debug-tc 选项，用于提升类型比较的调试。
- 引入--enable-debug-type-canonicalization 配置选项,更好地跟踪类型(反)序列化中的问题。
- 在 IR 中改正了关于规范化类型传播的文档。
- 对规范化逻辑进行了优化，避免错误规范化不应该处理的类型。
- DWZ 读取器现在可以处理.dynamic 段中的 SHT_PROGBITS 部分。
- 在确认环节，添加对传播规范化类型启用时避免取消机制的支持。

- 增强了与编译时（Compile Time Function）CTF 测试相关的支持。
- 对于来自__kcrctab 的 CRC 值，增加了支持。
- 添加了 abidiff 的--debug-tc 调试选项。
- 强化了利用 ODR & DWZ 的 DWARF 读取器和语言程序的稳定性。
- 将前端作为主要构件加以重视。
- 更新了 CTF 测试。
- 支持克隆联合体的数据成员。
- 解读 DWARF 5 的 addrx 位置。
- 避免规范化一个已经被“确认”的传播规范化类型。
- 通过文件扩展名添加了逻辑以检测文件类型。

5.3.14. multipath-tools：多路径存储

- 新增命令 del maps 刷新映射表并删除不识别设备
- 配置文件新增 protocol 子部分，实现针对不同存储协议进行配置和属性设置，从而为不同存储协议提供最佳配置。
- /run 替换/dev/shm
- 当使能 remove_local_path 时，不在 nvme 设备上创建 dm 设备
- 在执行 trasport pathinfo 之前增加针对 remove_local_disk 的检查

5.3.15. mesa：图形加速

- 新增特性 virtio-gpu 支持硬件编解码（H264、H265）

5.3.16. openssl：安全传输

- 支持内核模块国密签名功能，openssl 上层包需要合入相关补丁
- 支持兆芯国密支持 SM2、SM3、SM4
- 增加 TLCP 的支持。
- 支持 sm2utl，返回值与其他模块保持一致，支持默认 ID
- 优化了 openssl gdst 的命令参数为 G 的问题
- 为了修复 CVE-2023-0286 导致 libcrypto.so.1.1.1f 中 GENERAL_NAME 的成员变量 x400Address 指向类型由 ASN1_TYPE 变成了 ASN1_STRING,这两类型本身是不兼容的。

5.3.17. pam：用户认证

- pam_exec 实现了 quiet_log 选项。
- pam_mkhomedir 在/etc/login.defs 中增加了对 HOME_MODE 和 UMASK 的支持。
- 为提供的库增加 pkgconfig 文件。
- 增加了--with-systemdunitdir 配置选项来指定 systemd 单元目录。
- 增加了--with-misc- conf-bufsize 配置选项来指定 libpam_misc 的 misc_conv()函数中的缓冲区大小，将该参数的默认值从 512 提高到 4096。
- pam_faillock:增加了不设置 pam_fail_delay 的 nodelay 选项
- 扩展 libpam API 与 pam_modutil_check_user_in_passwd 功能。
- configure 添加了--disable-unix 选项来禁用 pam_unix 模块的构建。

- pam_faillock 将/run/faillock/$USER 权限从 0600 修改为 0660。
- pam_limits 增加了对 nonewprivs 项的支持。
- pam_pwhistory 添加 SELinux helper。
- pam_unix 和 pam_usertype:避免某些定时攻击。
- pam_wheel 在 getlogin 失败的情况下实现 PAM_RUSER 回退。
- 删除了 pam_cracklib 模块，使用 pam_passwdqc(来自 passwdqc 项目)或者 pam_pwquality(来自 libpwquality 项目)。
- 移除已弃用的 pam_tally 和 pam_tally2 模块，使用 pam_faillock 代替。
- pam_env 不赞成读取用户环境，将被删除。
- pam_motd 按照用户和组筛选 motd。

5.3.18. shadow：用户密码

- 读取用户输入由 fgets 转换成 fgetc,避免截断
- 增加 zh_HK 的支持
- UID 唯一性增加 flag， off 状态 -u 参数默认 getpwuid，on 状态，-u 使用 uid_used。

5.3.19. tuned：系统调优

- 更新 mssql 配置文件
- 增加 transparent_hugepage.defrag 参数；
- sysctl 设置直接写到/proc/sys，避免执行 sysctl --system，减少开销；

- 删除了 sap-hana-vmware profile 文件，不再需要的配置文件会对用户造成疑惑；
- 更新 virtual-host profile 文件，增加 cpu 分类下的 force_latency 参数；
- 增加了 accelerator-performance 配置文件；
- 更新 sap-hana 配置文件，对 sysctl 和 schedular 参数设置进行了更改；
- 更新 latency-performance 配置文件，对 scheduler、sysctl 相关参数进行了更改；
- 增加了 intel-sst 的 profile 配置，用于 intel 某场景调优。
- 增加了 optimize-serial-console 配置。
- throughput-performance 配置文件中增加了对 AMD 和 Marvell Thunder X 处理器的参数设置支持；
- 增加 spectrumscale-ece 配置文件
- scheduler 类别下增加了 default_irq_smp_affinity、perf_process_fork、perf_mmap_pages 等选项的支持。
- 增加了 postgresql 配置文件
- bootloader 增加了对 rpm-ostree 的支持。
- realtime 默认值更改为 isolcpus=domain,managed_irq,X-Y。
- 改进了 realtime 的验证函数，如移除了 disable_ksm 的函数调用
- scheduler 允许从特定 cgroup 中排除进程；
- 移除 python-configobj 依赖，切换到内置的 configparser；
- 针对 Centos 对 SPEC 文件进行了更新，不需要安装 subscription-manager；

- 增加 OpenShift 配置文件
- disk 磁盘调优参数增加了对 nvme 的支持；
- cpu 调优扩展了 cstate force_latency 语法来支持跳过零延迟；
- net 增加了对 txqueuelen 的支持；
- bootloader 在 s390(x)上从 BLS 中删除 TuneD 变量；
- daemon 在 systemd 失败时不执行完全回滚；
- 增加了 isolated_cores 规范中对引号的支持；
- 增加了 calc_isolated_cores 函数，并在一些 tuned 文件中增加 isolated_cores 初始自动设置。

5.3.20. util-linux：系统工具

- libblkid 工具优化：

  (1)对 JMicron 使用校验和；

  (2)优化 jm_checksum 和 le_to_cpu 函数的使用；

  (3)清除 tab 缩进，改为空格；

  (4)nvidia_raid 验证超级块大小；

  (5)nvidia_raid 验证校验和；

- logger 工具优化：

  (1)header 大小改变时重新分配缓冲区；

  (2)优化标准输入时--size 选项的使用；

- chfn 工具优化

(1)在单独的一行中对每个字段进行读行提示；

(2)对变量进行初始化，在读取标准输入前进行标准输出刷新；

- chsh 工具在读取标准输入之前进行标准输出刷新；
- login 工具调用 vhangup 后恢复 tty 大小；
- vipw 工具在获取结果之前进行标准输出刷新。

5.4. 安全

5.4.1. security-tool：

- 在 sshd 的默认配置项中删除已弃用的选项 RSAAuthentication 和 Rhosts RSAAuthentication 选项
- 删除 sshd 中业界公认的不安全算法 sha1
- 添加多种安全算法
- /etc/ssh/sshd_config 配置文件中增加 PubkeyAcceptedKeyTypes HostKeyAlgorithms 的配置项

5.4.2. shim：

- 增加对可信计算 3.0 支持，基于鲲鹏、海光平台支持在启动阶段调用 tpcm 可信设备模块，与可信计算模块系建立安全通信；
- 支持 RSA/国密在 x86/arm/loongarch64 平台上的安全启动，shim 中支持 SM3 和 SM2 算法；
- 新增支持支持 loongarch64 架构；
- 更新使用说明、配置指南和故障排除指南；

5.4.3. chpolicy：

- 新增兼容 selinux_policy32 和 33 版本

5.4.4. kysec-common：

- kysec 日志服务优化，日志元素标准化，提升日志并发的处理能力

5.4.5. kysec-daemon：

- 融合安全套件接口
- 应用联网管控改为黑名单模式，默认不管控，配置策略后进行管控
- 日志优化
- 添加软件包黑白名单 kdk 接口
- 添加应用执行控制 kdk 接口
- 添加软件防卸载 kdk 接口
- 添加内核模块防卸载 kdk 接口
- 添加进程防杀死 kdk 接口
- 添加文件保护 kdk 接口
- 修改使 securit-switch 切换状态后重启生效

5.4.6. kysec-sync-daemon：

- 融合安全套件接口
- 日志优化
- 应用联网管控改为黑名单模式，默认不管控，配置策略后进行管控
- kmod 修改使用 kdk 接口

5.4.7. kysec-utils：

- 融合安全套件接口
- 应用联网管控改为黑名单模式，默认不管控，配置策略后进行管控

- 日志优化
- 添加软件包黑白名单 kdk 接口
- 添加应用执行控制 kdk 接口
- 添加软件防卸载 kdk 接口
- 添加内核模块防卸载 kdk 接口
- 添加进程防杀死 kdk 接口
- 添加文件保护 kdk 接口
- 修改使 securit-switch 切换状态后重启生效

5.4.8. security-switch：

- 修改使 securit-switch 切换状态后重启生效

5.4.9. libsecurity1：

- 应用联网管控的默认配置改为黑名单模式
- 加入 kysec_sm 配置

5.4.10. libchkuid：

- 提供状态检查接口，可以通过配置开启或关闭检查相同 UID 的功能

5.4.11. security-reinforce：

- 安全加固功能升级：
- 提供等保三级、麒麟安全默认模板，等保三级共 46 个加固项；麒麟安全为麒麟推荐加固模板，共 70 个加固项；提供自定义模板，用户可针对 139 个加固项快速细粒度的自定义并加固，用户也可以根据大类（15 个大类）进行粗粒度的自定义和加固。提供简单易用的图形和命令行交互式工具，方便用户进行操作。
- 安全加固框架：

增加自定义参数功能，所有安全加固项支持自定义加固参数的修改，实现加固项灵活配置。
支持单项扫描、加固和还原，与以前的基于模板的扫描、加固、还原相兼容。
支持加固项公共行为合并单独处理
增加模板导入导出功能
增加非交互式命令行

- 安全加固项：
  增加加固项：
  开启审计机制
  设置审计存储阈值
  关闭系统不必要的端口
  限制 SSH 服务可访问源
  启用 SELinux
  限制用户使用计划任务
  管理 sudo 权限
  启用 sudo 日志
  设置 sudo 命令使用伪终端执行
  设置使用指定用户 sudo 提权需输入指定用户的密码
  删除无属组属主的文件或文件夹
  启动日志服务 rsyslog
  检查是否安装时间同步软件包
  设置系统时间同步
  检查空链接文件
  检查不安全组件
  检查可调试组件
  加强口令的密码算法
  禁止系统自动登录
  禁止 SSH 免密登录

设置守护进程的 umask 值

限制多重并发会话数

检查是否安装入侵检测工具 AIDE

检查文件完整性检测配置

设置登录后系统提示信息

5.4.12. rootca-gov-cn：

- 新增国家电子根证书管理工具，并提供开发接口

5.4.13. openssl：

- 增加支持兆芯 GMI 国密算法
- 回退支持海光 CCP 的补丁，改为 HCT

5.4.14. openssh：

- 支持国密算法 SM2、SM3、SM4

5.4.15. nettle：

- 支持国密算法 SM2、SM3、SM4

5.4.16. gnutls：

- 支持国密算法 SM2、SM3、SM4

5.4.17. rustcrypto-hashes：

- 增加 rust hash 算法开发库，支持 SM3

5.4.18. rpm：

- 增加软件包安装和卸载控制机制
- 修复安全开启时，更新软件包后特殊标记丢失的问题

5.4.19. libkysdk-security：

- 增加通用安全开发接口库

5.4.20. libkydima：

- 新增动态度量管理工具

5.4.21. lkrg-kyextend：

- 新增动态度量内核模块

5.4.22. usbguard：

- 增加用户交互窗口，提供开发接口

5.4.23. trousers-tcm：

- 新增 tcm1.2 软件栈

5.4.24. trousers-tcm-tools：

- 新增 tcm1.2 软件栈工具包

5.4.25. libtcmalg：

- 新增 tcm1.2 软件栈算法接口库软件包

5.4.26. libtpms：

- vTPM 支持国密算法 SM3

5.4.27. libkysec-tee：

- 新增飞腾 S2500 机密计算开发接口库

5.5. 容器、虚拟化

5.5.1. libvirt：

- 新增支持 loongarch64 以及龙芯虚拟机使用 host-model 启动方式。
- 对 qemuMonitorUnregister 加锁，防止 use-after-free 错误
- 新增支持 S5000c 处理器架构；

- 优化 domblklist 命令的输出；

5.5.2. lxc：

- on_error 处理增加逻辑，仅初始化 lock 失败时打印
- 优化旧逻辑，使用__do_free，避免释放内存错误
- 重构 selinux 标签的转换为共享模式
- 使用"__do_free "宏，而不是调用 "free "宏，以消除对内存泄漏的担忧
- 略增加 runtime_sock 目录的权限，提升为 0700
- 增加场景考虑，过滤 args 为空和未提供 rootfs 路径情况
- 变动策略为在 parent mounted 后建立 rootfs masked 路径
- 非 hierarchies 跳过 kill group 进程逻辑
- 增加 sw64 架构支持。
- 增加 lxc-attach 和 add-gids 选项
- 改正 lxc-attach --help 中输出，从 suffi 变更为 suffix
- 增加 loongarch64 架构支持
- 编译增加 yajl 支持。
- 在 getenv 后使用 ocihook

5.5.3. openvswitch：

- 优化 check_orig_tuple() 函数中的数据包筛选代码、提高性能
- 优化 reverse_nat_packet() 函数的 ICMP 报文的反向 NAT 处理代码，确

保在填充大于 127 字节的情况下的正确处理。

5.5.4. qemu：

- 飞腾 S5000c 新增支持 cpu 使用 host-model 启动
- 增加海光 CSV 加密功能
- 添加用于查询 virtio-blk 和 virtio-net 的 vring 参数的 api

5.5.5. virt-manager：

- 优化龙芯架构支持，主要是支持安装虚拟机、以及解决安装过程中不显示 virtio 网络设备网速的问题；
- 新增繁体翻译支持；
- 优化 virt-install 使用--install os 参数时的配置分支选择；

5.5.6. docker-engine：

- 新增 loongarch 架构支持
- 修改 docker 的默认启动参数，新增--iptables=false 参数关闭 docker 的 iptables
- docker 安装后默认不开机自启
- 适配 runc 安装路径改变，修改对 runc 的打包路径
- 增加策略在重启 docker 服务后清理 docker 残留 netns 文件
- 发送信号前不停止健康检查。
- 将 freezer.state 设置为 Thawed 以增加 freeze 几率。

- 当 docker manifast 中设置--insecure 且 Repository url 为 https 时，如果 docker 从 repo 源获取 response 数据失败，会将 url 转为 http，再次发起 get http 服务。
- 在 docker 移除挂载点时，使用 os.RemoveAll 代替 unix.Rmdir。
- edk2：
- 新增支持 TPM2 虚拟机启动可信引导
- 新增支持海光机密虚拟化硬件解决方案

5.6. 新增特性组件

5.6.1. openCL-SDK:异构计算开发 SDK

OpenCL™（开放计算语言）是一种开放的、免版税的标准，用于超级计算机、云服务器、个人计算机、移动设备和嵌入式平台中各种加速器的跨平台并行编程。OpenCL 大大提高了众多市场类别中各种应用程序的速度和响应能力，包括专业创意工具、科学和医疗软件、视觉处理以及神经网络训练和推理。

- OpenCL SDK。它汇集了开发 OpenCL 应用程序所需的所有组件：
- OpenCL Headers （include/api）
- OpenCL C++ 绑定 （include/cpp）
- OpenCL Loader
- OpenCL 实用程序库（include/utils）
- 它还包含对 OpenCL 开发人员有用的资源：代码示例（示例/）、文档（文档/）；

5.6.2. nettrace：网络工具

基于 eBPF 的集网络报文跟踪（故障定位）、网络故障诊断、网络异常监控于一体的网络工具集。可以跟踪报文在内核协议栈中的流转路径。

5.6.3. memstrack：系统诊断工具

一个内存跟踪工具，用于检测和诊断内存泄漏、内存使用情况以及内存分配问题。

5.6.4. etmem：多级内存存储

etmem 对内存数据进行分级，将分级后的内存冷数据从内存介质迁移到高性能存储介质中，达到内存容量扩展的目的，适用于对内存使用较多，且访问相对不频繁的业务软件，扩展效果较好，比如 MySQL、Redis、Nginx 等。

5.6.5. iodump：io 问题排查工具

iops dump 工具是利用内核 tracepoint 静态探针点技术实现的一个 io 问题排查工具。通过 iops dump 工具，我们可以获取每一个 IOPS（w/s 和 r/s）的详细信息，不仅包括 IO 请求的 size 大小，还包括 IO 请求的扇区地址，同时还包含 IO 请求的发生时间、读写的文件全路径、产生 IO 请求的进程、产生 IO 请求的系统调用和扩展 IO 类型等信息。这其中最具有特色的就是读写的文件全路径功能。简称其为 iodump。

5.6.6. pingtrace：网络问题诊断工具

是一个基于 ICMP 协议的网络时延探测工具，可供分析当前网络中的时延问题并确定问题边界。与 nettrace 不同的是，PingTrace 使用 C/S 架构，通过扩展 ICMP 协议新增时延探测协议，能完整的探测出一条数据链路中各环节的时延信息，便于快速发现问题边界。同时基于 CORE（Compile Once--Run Everywhere）为基础实现，保留了资源占用低、可移植性强等优点，还融合了 BCC 动态编译的特性，适合在生产环境批量部署应用。

5.6.7. spdk：高性能存储技术

提高数据存储系统的性能，提供了一套用户态的存储驱动，用于替代传统的内核态驱动。用户态驱动可以避免内核上下文切换的开销，从而提高 I/O 性能；使用轮询模式代替中断方式处理 I/O 请求。轮询模式可以减少中断处理的开销，提高 CPU 利用率；使用无锁数据结构和原子操作来减少锁竞争，提高并发性能；支持多核并行处理 I/O 请求，充分利用现代多核处理器的性能；支持异步 I/O 操作，允许应用程序在等待 I/O 完成时执行其他任务，提高系统整体效率；使用内存池技术，减少内存分配和释放的开销，提高性能。SPDK 适用于多种存储应用场景，如 NVMe-oF、iSCSI、vhost、NVMe、vHost-User 等。通过使用 SPDK，可以构建高性能、低延迟的存储系统，满足各种高性能应用场景的需求。

5.6.8. gazelle：高性能网络

Gazelle 实现了一套完整的 TCP/IP 协议栈，具有高性能、低延迟、高吞吐量的特点，可以满足高性能网络应用的需求。基于 dpdk、lwip 实现了高性能轻量协议栈能力，主要特性如下：

- 极致性能，基于区域大页划分、动态绑核、全路径零拷贝等技术，实现高线性度并发协议栈。
- 硬件加速，支持 TSO/CSUM/GRO 等硬件卸通用性（posix 兼容），接口完全兼容 posix api，应用零修改，支持 udp 的 recvfrom 和 sendto 接口。
- 通用网络模型，基于 fd 路由器、代理式唤醒等机制实现自适应网络模型调度，udp 多节点的组播模型，满足任意网络应用场景。
- 易用性（即插即用），基于 LD_PRELOAD 实现业务免配套，真正实现零成本部署。
- 易运维（运维工具），具备流量统计、指标日志、命令行等完整运维手段。

5.6.9. lasso：云计算身份认证

Liberty 联盟的单点登录协议(Single Sign On)实现库，包括 SAML2 和 SAML。

5.6.10. p7zip：压缩工具

可以将文件或者目录归档压缩为 7zip 格式， 提供了 7za 命令。

5.6.11. LZMA-SDK：压缩工具

LZMA-SDK 是 7-zip 项目的子模块，主要提供一个 lzma 命令,以及应用

中使用 lzma 压缩算法所需要的工具和库。

5.6.12. ElectricFence：C 语言调试工具

Electric Fence 是一种 malloc 调试器的库。用于 C/C++编程和调试。它使用系统的虚拟内存来检测软件何时超出 malloc 函数缓冲区的边界。它还将检测 free 函数释放的任何内存访问。

5.6.13. LeakTracer：内存泄露检测工具

LeakTracer 是一个小型的 C++内存泄露检测工具。在使用 LeakTracer 时，通过提供的 LeakTracer 脚本运行你的程序，它使用 LD_PRELOAD 在你的函数上层进行“重写”。如果你的平台不支持 LD_PRELOAD，则需要将 LeakTracer.so 对象文件加入到 Makefile 文件中，然后运行你的应用程序。

简单一点说就是，它是一个小型的内存申请释放分析工具，通过”重写”内存分配函数（new、delete、malloc 等），记录内存的分配和释放情况，记录申请内存调用堆栈。来达到内存泄漏检测的情况。

5.6.14. METIS：图数据处理

是一组用于串行图切分的软件包。在 METIS 中实现的算法是基于多层的递归对分，多层 k-way 和多约束。提供图切分算法库、命令及开发 API。

5.6.15. webbench：WWW 测试

用于基准 WWW 或代理服务器。使用 fork()模拟多个客户端，可以使用 HTTP/0.9-HTTP/1.1 请求。这个基准测试并非真实的，但它可以测试 HTTPD 是否真的可以在不关闭机器的情况下同时处理那么多客户机(尝试运行一些 cgi)。显示页/分钟和字节/秒。

5.6.16. aespipe：加密工具

用于 tar/cpio 和 loop-aes 的基于 aes 的加密工具。

5.6.17. QAT20：通信加速技术

英特尔通信加速技术提供加密和压缩加速功能，用于提高整个数据中心的性能和效率。此包为其硬件 2.0 驱动。

5.7. 其他方面

5.7.1. abrt：

- 新增 abrt-cli、abrt-desktop 两个子包
- 新增 abrt-console-notification 子包

5.7.2. accountsservice：

- 修改了源码，在默认过滤的用户列表（黑名单）里，添加 pcpqa 用户
- 改进了识别用户会话的贪婪算法
- 提供接口目录给 pkgconfig 配置工具

- 锁定状态目录，提高有私密性要求的 accountsservice 扩展的安全性
- 翻译更新

5.7.3. acl：

- 删除二进制中的 rpath 属性设置

5.7.4. aide：

- aide 组件新增 SM3 算法支持。

5.7.5. amanda：

- 添加安装依赖 sharutils

5.7.6. anaconda：

- 系统安装过程中，系统默认启动项由“/etc/machine-id+内核名称”改为产品名

5.7.7. apparmor：

- 修改 common/Make.rules 文件，使之可以正确的生成头文件
- 修改 utils/apparmor/tools.py 文件，cmd 时传入正确的参数

5.7.8. atril：

- 添加繁体中文翻译支持

5.7.9. atune-collector：

- 新增功能：应用配置下发特性相关,启用应用程序配置功能和配置备份功能

5.7.10. audiofile：

- 移除可执行文件的 rpath/runpath 属性值、提升安全

5.7.11. authd：

- authd 加密新增支持 SHA256 算法

5.7.12. autogen：

- 删除二进制中的 rpath 属性设置

5.7.13. bcc：

- 新增支持 loongarch 架构

5.7.14. bind：

- 添加 selinux-policy-targeted 依赖
- 由于 geoip 已转商用，删除与 geoip 相关的接口：dns_geoip_match、dns_geoip_shutdown、 dns_message_destroy；

5.7.15. blivet-gui：

- 优化繁体中文支持

5.7.16. brasero：

- 添加繁体中文翻译支持

5.7.17. brltty：

- 删除无用的兼容性库文件，删除了 brltty tcl-brltty，删除安装 libbrlapi.so。删除不合规范的字符

5.7.18. ca-certificates：

- certdata.txt 中删掉了不安全的证书。

5.7.19. caja-extensions：

- 增加繁体翻译

5.7.20. caja：

- 增加繁体翻译

5.7.21. catfish：

- 优化 svg 和 png 的搜索速度，
- 新增对 wayland 和 gnome shell 新版本的支持，
- 优化了首选项窗口布局，

5.7.22. ccid：

- 新增新设备支持
- 禁用 AlcorMicro-AU9520 读卡器的 USB 挂起
- 新增支持 Feitian R502 C9 4 卡槽
- 删除 The Kobil TriBank reader 扩展 APDU 功能

5.7.23. cdrkit：

- 编译依赖中不再需要 git 软件包
- 支持 sw64 架构

5.7.24. ceph：

- 将依赖 selinux-policy-base 改为 selinux-policy-minimum

5.7.25. checkpolicy：

- 避免传递空指针给 class_perm_node_init 中的 memset

5.7.26. check：

- 修改 check.h 文件模板，在原有的浮点数相等和不相等的宏定义中，添加了一些警告信息，强调了这些宏的使用范围受限，并建议开发者使用带有容差的版本；
- 将 web/install.html 文件的标题由 Users of Check 改为 Installing Chec k；
- 优化 START_TEST 宏的实现方式，使之看起来像有效的 C 代码

5.7.27. clang：

- 增加编译参数-DCLANG_LINK_CLANG_DYLIB=ON 和-DBUILD_SHARED_LIBS=OFF
- 增加对.a 静态库文件的打包
- 移除可执行文件的 rpath/runpath 属性值、提升安全

5.7.28. clevis：

- 支持 tpm2-tools 4.x；
- 支持 initramfs-tools 解锁工具
- 添加了 clevis luks list 命令；
- 对 initramfs-tools 支持进行了改进；
- 改进了在启动时解锁多个 LUKS 设备的支持
- dracut：为 hostonly-cmdline 和 tang 绑定添加 rd.neednet
- luks：添加 clevis luks edit 命令，添加 clevis luks report，添加 clevis luks regen 命令
- askpass：将 systemd 目录监视条件更改为 DirectoryNotEmpty
- 为 clevis luks bind 引入 -y（假设是）参数
- 允许用户在绑定时指定令牌 ID
- pins/tpm2：添加对 tpm2-tools 5.X 的支持
- 添加 clevis luks pass 命令

- 添加对二进制密钥文件的正确支持
- systemd：去除对 ncat 的依赖
- 改进 bind 时 tang 声明的验证
- 默认的 tang JWK thumbprint 现在是 SHA-256，弃用了 SHA-1
- 确保 clevis-luks-bind 中的配置是有效的 JSON
- 添加 clevis luks unlock 的测试选项
- luks：使用 bash 的内置序列表达式替换 seq

5.7.29. cmake：

- 增加 loongarch64 架构支持
- 优化软件包构建速度

5.7.30. cockpit-appstream：

- 修改汉化翻译，瘦逻辑卷为精简逻辑卷
- 为 loongarch 架构添加安装依赖 libvirt-daemon-kvm

5.7.31. color-filesystem：

- 增加对 loongarch 架构的支持
- 增加对申威架构的支持

5.7.32. coreutil：

- 在存在远程（例如 NFS）绑定挂载（mount --bind）的情况下，df 命令输出了重复的远程装载

- 优化 wc()函数，确保更新文件偏移量
- 优化 setenv，对 malloca()函数返回 NULL 的情况进行兼容，防止 setenv 工具 crash。
- 更新 od 工具-S 参数的使用说明

5.7.33. cracklib：

- 可执行文件中删除 runpath 以及 rpath

5.7.34. cronie：

- 并发执行 systemctl restart crond，systemctl reload crond 时，低概率导致 crond 进程退出的问题

5.7.35. crypto-policies：

- 用于检查 NSS 配置的 perl 脚本转为 python 脚本；
- 对 crypto-policies 提供的配置中的异常情况添加更多详细说明；
- 向 NSS 策略支持 SM3

5.7.36. curl：

- 在 tests 用例洪禁用 valgrind

5.7.37. cyrus-sasl：

- 使用 gdbm 替换 libdb，

5.7.38. dietlibc：

- 安全增强，增加 BIND_NOW 和 PIE 编译参数

5.7.39. dmidecode：

- 更新到 3.3 版本：

(1)允许在环境中重写构建设置；

(2)在 arm64 架构的/dev/mem 上不使用 memcpy；

(3)仅在 x86 架构的/dev/mem 上扫描入口点；

(4)支持 SMBIOS3.3.0，包括新的处理器名称、新的端口连接类型以及新的存储器设备厂商、类型和技术；

(5)将 bios 修订版、固件修订版和系统 sku 编号添加到-s 选项中；

(6)使用合适的缓存大小单位；

(7)基于总线宽度和对等点解码系统槽；

(8)优化 Redfish 主机名打印长度；

(9)修改 TPM 表输出的格式设置；

(10)增加 PCIe SSD 系统插槽信息；

(11)防止因无效的处理器电压而阻塞。

- 更新到 3.4 版本：

(1)支持 SMBIOS 3.4.0，包括新的内存设备类型、新的处理器升级、新的插槽

类型和特性、内存模块扩展速度的解码、新处理器特性和新的处理器 ID 格式；

(2)支持 SMBIOS 3.5.0，包括新的处理器升级、BIOS 特性、新插槽特性、新的板载设备类型、新的定点设备接口类型和新的记录类型；

(3)解码 194、199、203、236、237、238 和 240 HPE OEM 记录；

(5)忽略已卸载内存模块的详细信息；

(6)quiet 模式下不显示原始 CPU ID。

- dmidecode 命令新增--compat-uuid 选项，使用 SMBIOS 2.6 规范的兼容 uuid 格式。
- 新增支持 loongarch、sw64 架构；

5.7.40. docbook2X：

- 增加-h 及-v 功能，分别用于查看命令参数及当前软件包版本号

5.7.41. docbook-style-dsssl：

- 处理空链接文件路径:/usr/share/sgml/docbook/dsssl-stylesheets

5.7.42. docker-proxy：

- 对 loongarch64 架构移除不支持的 build=pie 参数

5.7.43. dovecot：

- 添加安装依赖 dovecot-help；

- 删除二进制中的 rpath 属性设置。

5.7.44. dyninst：

- 增加 aarch64 支持

5.7.45. ebtables：

- 删除无效的软连接文件/usr/lib64/libebtc.so；

5.7.46. edac-utils：

- 执行 systemctl stop edacd 停止服务时，去掉不支持的--unload 操作，避免服务停止失败

5.7.47. efibootmgr：

- 添加对 LoongArch 的支持
- 为--index（-I）选项添加了缺失的短选项处理
- get_entry 函数：在到达列表末尾之前，如果找到了条目，则返回该条目
- 新增命令选项：

  -f | --reconnect 加载驱动程序后重新连接设备

  -F | --no-reconnect 加载驱动程序后，不要重新连接设备

  -I | --index number 创建条目时，将其以指定的引导顺序插入（默认值：0）

  -r | --driver 操作驱动程序变量，而不是启动变量

5.7.48. efivar：

- 正确检查 mmap 返回错误；

5.7.49. elfutils：

- 子包拆分，将 eu-objdump, eu-readelf, eu-nm 移动至新增的 elfutils-extra 子包。

5.7.50. emacs：

- 增加 emacs desktop 文件中文翻译

5.7.51. engrampa：

- 添加 desktop 文件及程序界面上缺失的繁体中文翻译

5.7.52. environment-modules：

- 删除不存在的 man 手册文件软链接

5.7.53. eom：

- 增加繁体中文的支持；

5.7.54. esc：

- 删除二进制文件的 rpath 属性

5.7.55. ethtool：

- 新增了读取 Intel 2.5G igc 和 Broadcom bnx 网卡驱动寄存器信息的功能

5.7.56. evolution-data-server：

- 删除二进制文件的 rpath 属性

5.7.57. exiv2：

- 删除二进制文件的 rpath 属性

5.7.58. extra-cmake-modules：

- 升级版本到 extra-cmake-modules-5.59.0-2.ky10

5.7.59. fakechroot：

- glibc 2.28 后支持 startx,fakechroot 相应支持 startx

5.7.60. fcitx-chewing：

- 增加繁体翻译

5.7.61. fcitx-configtool：

- 增加繁体翻译

5.7.62. fcitx：

- 增加繁体翻译

5.7.63. file：

- 增加对 loongarch64 的支持

5.7.64. firefox：

- RequestDestination::Script 对于 nsHttpChannel MIME 类型不做检查，从而引起脚本可以运行
- 在 libexpat 库中，攻击者通过网络攻击的方式，利用精心制作的 xml 文件，触发漏洞的 xml 文件需要达到 GB 级别，导致 xmlparse.c 中的 storeAtts 函数中左移 29 个(或更多)位置可能会导致 realloc 行为不端(例如,分配的字节太少,或仅释放内存)。漏洞主要威胁系统的可用性

5.7.65. firewalld：

- 优化繁体字支持

5.7.66. fprintd：

- 将 fprintd 包的卸载脚本中的关闭指纹的相关调用加了调用条件，即只有当前系统已经开启了指纹才需要关闭该特性

5.7.67. freeradius：

- 删除可执行文件和库文件中的 rpath 和 runpath

5.7.68. freerdp：

- 安装依赖增加 systemd-pam

5.7.69. fuse：

- 根据当前 glibc 版本条件性定义 closefrom 函数；
- 添加 test 文件夹，用于添加测试用例；

5.7.70. fwupd：

- 更新 fwupdmgr --help 中--clear-history 参数的中文翻译

5.7.71. gc：

- 新增 loongarch 架构支持

5.7.72. gdbm：

- 安装和卸载 gdbm-devel 包时有告警信息，安装 devel 时需要安装 help 包。
- 当数据库中无 key-value 时，dump 出数据时报错，增加相应判断，如为 0 不进行 dump。

5.7.73. genwqe-tools：

- gettid 改为 defs_gettid

5.7.74. git：

- 新增 git archive --add-file 等功能
- 已放弃对已弃用的 PCRE1 库的支持
- 分离 git-core 子包，将 git 依赖最小化

5.7.75. glade：

- 删除旧版本动态库

5.7.76. glassfish-hk2：

- 由于 openjdk 升级删除了 ClassPath.java，需要更换 import 路径。

5.7.77. glew：

- 在说明文件 README.md 中增加 glew 的描述

5.7.78. gnome-calculator：

- 优化繁体中文支持

5.7.79. gnome-disk-utility：

- 优化繁体中文支持

5.7.80. gnome-packagekit：

- 优化繁体中文支持

5.7.81. gnome-shell：

- 删除二进制文件的 rpath 属性

5.7.82. gnome-user-docs：

- 修改 License:CC-BY-SA 为 License:CC-BY-3.0。
- 增加磁盘相关的用户帮助手册信息；

5.7.83. gnome-vfs2：

- 解除对 gamin 的依赖

5.7.84. gnu-efi：

- 同源支持 loongarch64 与 mips 架构

5.7.85. gnulib：

- 更改编译依赖 java 的版本，从 1.3 改为 1.8

5.7.86. gnupg2：

- 添加编译依赖 gnutls-devel 以支持 TLS

- 优化 parse_ber_header、防止出现整数溢出问题

5.7.87. golang：

- 引入 amd64 架构 md5 优化补丁:对 amd64 架构下 md5 汇编文件进行改写，可以实现速度提升约 9%左右。

5.7.88. gperf：

- 启用生成本地化页面的支持

5.7.89. graphviz：

- 增加 loongarch64 架构
- 去除 elf 文件中的 rpath 属性，提升安全

5.7.90. grep：

- 优化 grep 查询效果展示

5.7.91. groff：

- 新增-x11 子包

5.7.92. grub2：

- 默认 disable 掉 grub-boot-success.service 服务

- 禁用 BLKID 缓存使用
- 避免错误地探测 ext2 文件系统
- 移除 installkernel 和 installkernel-bls 脚本
- 在 grub-core/disk/diskfilter.c 文件中对 calloc()的结果为 NULL 进行检查
- 在 grub-core/kern/buffer.c 文件中的 grub_buffer_free()函数中，添加对入参为 NULL 的判断;
- 在 grub-core/disk/diskfilter.c 文件中的 grub_diskfilter_make_raid 函数中，针对入参 nmemb 大于 1024 的情况返回 NULL,即不支持创建具有超过 1024 个磁盘的 RAID 阵列
- 在 grub-core/loader/linux.c 中，确保 newc 路径名以 NULL 结尾
- 在 grub-core/term/i386/pc/vga_text.c 中，防止越界写入 VGA 文本缓冲区
- 在 grub-core/osdep/linux/hostdisk.c 中，根据磁盘扇区大小来修改 sysfs 的扇区大小
- 在 grub-core/net/bootp.c 中，添加对调用 grub_netbuff_push()函数后的返回值的检查
- 在 grub-core/fs/iso9660.c 中，避免读取超过输入边界；防止在延续区域开始时跳过 CE 或 ST；防止读取超过系统使用区域的末尾；添加检查以防止无限循环
- 在 gentpl.py 文件中，从.img 文件中删除.interp 段
- 在 grub-core/font/font.c 文件中，对 max_char_width 或者 max_char_height 为负数的情况加判断；将 null_font 的地址赋给 unknown_glyph 的 fon

t 成员；在 ascii_glyph_lookup 函数中调用 grub_malloc（）函数后的返回值添加检查

- 不加载 grub.cfg 时跳过验证

5.7.93. gstreamer1-plugins-good：

- 去除 libgstshout2.so 的 rpath 属性

5.7.94. gvfs：

- 删除二进制文件的 runpath/rpath 属性值
- kylin 设备管控需求合入
- 安全套件 WINCE 管控优化代码

5.7.95. hardinfo：

- 设备信息不显示硬盘厂商信息；
- 设备系统信息处显示 CPU 最大速率为零；
- 龙芯架构下，系统信息里面无法识别主板信息；
- 系统信息下 PCI 设备中 Link Width 的数据显示有误；
- 系统信息中对应硬盘 S.M.A.R.T Attributes 中的 value 信息实际显示的是 Raw_VALUE 信息；

5.7.96. harfbuzz：

- 支持 GB18030-2022

- 去除 elf 文件中的 rpath 属性，提升安全

5.7.97. haveged：

- 安装后默认使能 haveged 服务

5.7.98. hdparm：

- 解码使用 id[69]更多 bit 比特。
- 允许从环境中传递自定义 LDFLAGS。
- 修改 dco-identify 最大扇区。
- 支持 ioSafe Solo 与 jMicron 桥接。
- 处理编译问题，增加静态编译。
- 新的--sanitize-overwrite-passes 标志。

5.7.99. help2man：

- 启用宏 nls，增加编译依赖 perl-Locale-gettext，启用生成本地化页面的支持

5.7.100. http-parser：

- 增加了 url 连接端口为空的默认处理功能

5.7.101. hwdata：

- 更新 PCI、USB 和供应商 ID；

- 许可证合规性整改。

5.7.102. hyperscan：

- hyperscan 新增 loongarch64 架构支持；

5.7.103. ibus-table：

- 在 os.makedirs 中添加 exist_ok=True 以避免因竞争条件而失败

5.7.104. icu：

- 增加支持 loongarch64 架构

5.7.105. imlib2：

- 删除 imlib2 id3tag-loader 以避免 libid3tag 问题

5.7.106. imsettings：

- 添加缺失的繁体中文翻译

5.7.107. initial-setup：

- 不要调用已移入安装键盘任务的任务。
- 从 Makefile 中删除未使用的 PREFIX 变量。
- 将多 TTY 处理程序中的一些 USB 控制台列入黑名单 。
- 将缺少的分支配置添加到清单文件。

- 删除对 python3-libreport 的过时依赖。
- 删除 tmp 中翻译仓库的硬编码名称。
- 使用本地化存储库添加 po-push .
- 使用新的 DBus 支持来读取 kickstart 文件。
- 使用新的 po-push 代替 Zanata.
- 适应本地化模块的变化。
- 运行本地化模块的安装任务。
- 运行 DBus 插件的安装任务。
- 运行 Timezone 模块的安装任务。
- 在规范文件中使用宏满足 Python 3 的要求。
- spec 文件移除旧的预脚本：该脚本防止在升级或包移除过程中出现死锁问题，通过在预处理阶段关闭和禁用初始设置服务来实现。
-
- intel-cmt-cat：
- 修改了 "pqos/pqos.8" 和 "rdtset/rdtset.8"两个文件，调整了其中的日期和网址，以确保 man 页面中的相关信息是准确的

5.7.108. ipmitool：

- 申请内存时，指定的内存长度不正确

5.7.109. iptstate：

- 规范 License 名称

5.7.110. ipxe：

- 允许启用或禁用使用 PeerDist 内容编码
- 允许指定 PeerDist 托管的缓存服务器
- 按照 UEFI 规范设置 EFI_SIMPLE_NETWORK_RECEIVE_MULTICAST 位
- address>/boot.ipxe 中带有冒号时，无法正确解析 url，导致引导失败问题。
- 允许使用 IPV6 地址来引导;
- 添加对 Broadcom NetXtreme-E 适配器的驱动程序支持;
- 为所有的引导服务添加调试功能;
- 添加了对 USB 大容量存储设备的支持;
- 禁用 ARM64 EFI 构建;
- 禁用 MD5 作为 OID 可识别算法;
- 默认支持的最低版本 LTS 协议从 LTSV1.0 升级到 LTSV1.1;

5.7.111. iSulad：

- 增加为容器设置用户命名空间功能
- 当 userns-remap 开启时，即打开设置容器用户命名空间功能，增加支持设置 isulad 根路径功能
- 清除关于处理 http 请求头代码。
- 重构 spec 模块中 mount 解析代码。

- 对非 oci 镜像支持 wait 子命令。
- 对 image 服务支持 restful 模式。
- 适配 selinux 打开场景。
- 适配 bionic libc，提高 lcov 覆盖率。
- 清理 grpc 客户端冗余代码，并整理格式。
- 重构 util_getgrent_r 和 util_getpwent_r。
- 增加如果未找到控制器，则不创建 isulad 目录逻辑。
- 在 init_label 中移除检查参数 label_opts。
- 如果用户为 dev shm 设置了挂载，则不挂载可共享的目录。
- 为 libhttpclient.so 和 libisulad_tools.so 添加读取和执行权限。和 libisulad_tools.so 的读取和执行权限，以便加入 isula 组的非 root 用户可以正常使用 isula 命令。
- 适配 openssl 3.0
- 通过 tm_gmtoff 计算时区。
- 变更 libisulad_tools.so 文件权限：
- 为容器添加 hostname。
- 在等待 fifo 退出时使用 epoll 代替 select。
- 添加 lcr 和 clibcni 组件依赖范围：
- 确保被 kill 掉的 pid 不为负数。
- 增加逻辑若添加设备映射器设备失败，则移除 mnt 指针。
- 关于 isulad create 命令新增--rm 选项。

- 设置 inspect 容器超时时间。
- 在 merge 网络时检测文件系统。
- 增加 shim 等待所有子进程逻辑。
- 当执行 run 命令且设置 rm 选项时，增加删除已停止容器的 fifo 目录逻辑。
- 确保 isula exec 继承 create 的配置。
- 支持 pull 镜像时携带 digest。
- isulad-shim 支持异步执行超时。
- 增加进程失败检测。
- 支持当运行时为 runc 时 isula update 操作。
- 支持为 pod 设置 privilege 权限。
- 增加大页限制支持。
- 在 OCI 规范中增加有效和允许的上限类型。
- 增加 execSync 执行异常信息处理。
- 当 shim_created 完成释放 timeout 对象。
- 重构远程 ro 代码。
- 转换 lcr start/exec 请求结构体。
- 增加逻辑确保在关闭文件描述符前 isulad_io 不为 NULL。
- 当使用 kata 运行时时，禁用 exec 的超时限制。
- 重构 rt_isula_exec 和 shim 日志相关代码。
- 添加了对容器健康检查的限制。
- 限制 ExecSync 响应体大小。
- 防止使用不安全的 isulad tmpdir 目录。

- 使用宏控制插件开关。
- 处理 proxy 及 mask 信息。

5.7.112. itstool：

- 更新了 DocBook 关键字元素。
- 在使用--join 模式时，应用了通过-i 传递的 ITS 文件。

5.7.113. jboss-jaspi-1.1-api：

- 升级到 1.0.2 版本

5.7.114. jetty：

- 限制 ByteBufferPools 池的总字节数
- org.apache.filex:org.OSGi.foundation:jar 中 java.base 类的 OSGi 版本与 java9 上的新规则冲突
- HandlerCollection.addHandler 缺少同步
- 内存不足错误：GZIPContentDecoder 中的 Java 堆空间
- 新会话无效时发送的 JSESSIONID 重复
- 在终止 websocket 客户端后永远关闭_等待套接字状态
- 如果出现不可用时，则停止服务器
- 将 SslContextFactory 拆分为客户端和服务器。
- java.security.acl.Group 已弃用，并标记为要删除

5.7.115. jffi：

- 新增支持 loongarch64 架构

5.7.116. jnr-ffi：

- 删除冗余宏 pkg_vcmp
- 新增支持 loongarch64 架构

5.7.117. js-jquery：

- toArray()新增支持将 jQuery 对象转换为原生 DOM 对象的数组
- offsetParent()新增支持元素的 offsetParent 节点获取；

5.7.118. jsoncpp：

- 优化生成 pkg-config 文件时对于绝对路径的处理；

5.7.119. json-c：

- 避免无害的无符号整数溢出
- 删除旧的 so 文件（libjson-c.so.4()(64bit)）
- 删除预译开发中的取消链接文件：添加 pretrans 阶段的删除无用软连接的脚本。
- 启用 check test。

5.7.120. kata-containers：

- kata shimv2 增加对 iSulad 支持
- shimv2 以整数字节顺序编写退出代码，以适应 iSulad
- 增加 agent 进程 timeout 逻辑
- 将超时移至停止容器进程，由于该处逻辑仅用于停止容器进程以支持 shim v2
- 关闭 GO111MODULE
- kata-runtime 模块在创建容器和操作网络前，增加检查文件大小逻辑
- 修改 configuration-qemu.toml 中 hypervisor_params 参数
- 调用 blockdev-add 时使用 host_device 驱动
- 修改 runtime 模块构建 flags
- 添加 qmp 执行超时机制
- 适配 qemu 6.2 移除 kernel_irqchip
- 修改 MG 信息
- 更新 kata-containers 微内核 config 问题值 5.10.0

5.7.121. kexec-tools：

- 增加了 arm64 的 serial 打印选项，使其能重定向打印输出到串口；
- 增加了对 loongarch64 和 SW_64 的架构支持；
- 增加“mem=”参数，用于指示捕获内核启动时的内存区域。
- 删除在调用 xmalloc 和 xrealloc 之后永远不会满足的条件;
- 修改函数 uImage_arm64_probe 的返回值，使其更加明确的表达对应含义；

- 添加对处理 zlib 压缩（Image.gz）镜像文件的支持；
- 增加 x32 做为 x86_64 的子架构并且针对 x32 不使能-mcmodel=large 参数；
- 代码优化，在指针之前将 int 强制转换为 uintptr_t 以避免警告；
- 更新 vmcore-dmesg 的用户手册 man page；
- 增加 exec-live-update 参数，用于在存储实时更新所需要的状态后，执行当前加载的 xen 镜像；
- 增加 load-live-update 参数，用于加载新内核以覆盖正在运行的内核；
- 更新--status 的说明，明确返回值的定义；
- 增加 serial=STRING 参数，增加了 arm64 的 serial 打印选项，使其能重定向打印输出到串口。

5.7.122. kiwi：

- packagemanager 中新增 microdnf 选项；
- 新增 s390 SLE15 集成测试；
- 构建状态帮助显示信息样式更新；
- build_status 中新加入模块：Virtualization:Appliances:SelfContained:universal
- 新增对 openEuler 系统的构建，设置用户、组等特性；
- 新增构建使用 rsync 链接；
- 重构 grub2 安装功能，包括 secure boot install 等

5.7.123. kmod：

- 将/usr/local 添加到配置文件的搜索路径中，这使它更容易在不覆盖发行版文件的情况下进行本地安装；
- 对测试套件进行了其他改进，因此无论使用何种配置，我们都可以可靠地使用它：现在，如果我们没有构建依赖项，测试将跳过。
- 使用 libzstd 将 Zstandard 添加到支持的压缩格式中（pass--with zstd to configure）；
- 忽略格式不正确的内核命令行，例如其中有“ivrs_acpihid[00:14.5]=AMD0020:0”选项；

5.7.124. ksh：

- 去除 ksh-help 包，将该包的内容合并到主包 ksh（ksh 主包 provides ksh-help 包），并且新增 chkconfig 依赖

5.7.125. kylin-computer-viewer：

- 添加缺失的繁体中文翻译
- 添加操作系统免责声明港澳地区语言版本支持
- 修改操作系统版权信息年份至 2024 年

5.7.126. kylin-control-center：

- 为具有相同 UID 的用户在控制面板合并显示
- 麒麟蓝色主题使用 gtk 主题蓝色图标
- 添加繁体中文翻译支持

5.7.127. kylin-indexhtml：

- 修改更新“银河麒麟高级服务器操作系统 V10 简介”文本信息网页繁体翻译

5.7.128. kylin-menu：

- 繁体中文内容优化

5.7.129. lame：

- 新增申威架构支持

5.7.130. lapack：

- 添加安全编译选项“-D_FORTIFY_SOURCE=2”,启用强化的安全性检查机制
- 增加软件包 debuginfo 的生成

5.7.131. leveldbjni：

- 优化安全编译选项重编

5.7.132. libaio：

- 增加安全编译选项 D_FORTIFY_SOURCE

5.7.133. libcgroup：

- 新增支持申威架构

5.7.134. libdb：

- 在__check_lock_fn 接口中新增设备 id 检查；
- 新增支持申威 64 位平台；
- 新增编译依赖 BuildRequires：java-1.8.0-openjdk-devel；

5.7.135. libdnf：

- 新增 loongarch 和 sw_64 支持

5.7.136. libdrm：

- 删除二进制文件的 rpath 属性

5.7.137. libdvdnav：

- 新增 dvdnav_open2 接口，支持日志调试模式打开 dvd 文件对比
- 新增信息获取函数接口,dvdnav_get_number_of_angles、dvdnav_version
- 处理无序的 ADMAP 条目阻塞回放
- 增强损坏光盘的随机播放模式

5.7.138. libdwarf：

- 支持 DWARF5 rnglists 和 loclists，并通过设置 dwarf_set_de_alloc_flag(0) 来提高性能；
- 增加了对损坏的 DWARF 的检查功能，优化了 DWARF 表达式运算符的打印；

- 增加了属性/表单类使用和属性/表单使用的摘要信息；

5.7.139. libEMF：

- 删除二进制文件的 rpath 属性
- 增加 loongarch64 架构支持

5.7.140. libexif：

- 据，而不需要额外的执行权限。

5.7.141. libfastjson：

- 新增 API 接口 fjson_object_get_uint()、fjson_object_array_del_idx()；

5.7.142. libgcrypt：

- 为 AES 添加 GCM 和 CCM 到 OID 映射表。
- 使压缩点的 keygrip 计算生效。
- 为 Camellia 添加 x86_64 VAES/AVX2 加速实现。
- 为 AES 添加 x86_64 VAES/AVX2 加速实现。
- 在 PPC 上为 GCM 模式添加 VPMSUMD 加速。
- 强化 MPI 条件代码以防止 EM 泄漏。
- 强化 Elgamal 通过引入指数模糊。
- 为 ECDSA 验证操作检查公钥。

- 确保 gcry_get_config (NULL) 返回以空字符结尾的字符串。
- 添加新的测试驱动程序以允许独立的回归测试。
- 如果负 MPI 与 sexp 扫描函数一起使用，则返回错误。
- 在随机和 KDF 函数中检查操作 FIPS。
- 为更好的 LTO 支持改进汇编器检查。
- 支持没有 posix_spawn 的旧版 macO
- 为 s390x/zSeries 添加优化的密码和哈希函数。
- 使用硬件比特计数函数（当可用时）。
- 更新 DSA 函数以匹配 FIPS 186-3。
- 为 CMACs 和 KDFs 添加新的自测。
- 为 OFB 和 GCM 模式添加批量密码函数。
- 新的和扩展的接口：新曲线 Ed448、X448 和 SM2、新密码模式 EAX、新密码算法 SM4、新哈希算法 SM3。
- 新哈希算法变种 SHA512/224 和 SHA512/256，Blake-2 算法、新 SHA 512 变种、SM3 和 GOST 变种的新 MAC 算法。
- 新的便利函数 gcry_mpi_get_ui。
- gcry_sexp_extract_param 了解新的格式说明符,直接存储到整数和字符串。
- 新函数 gcry_ecc_mul_point 和 Curve448、Curve25519 的曲线常量。
- 新函数 gcry_ecc_get_algo_keylen。
- 新的控制代码 GCRYCTL_AUTO_EXPAND_SECMEM，允许扩展安全内存区域。
- 为 Aarch64 添加优化实现。

- Poly1305 和 ChaCha 的更快实现。
- 使用 AES-NI 改进 AES-XTS 的使用（速度提高 6 倍）。
- 为 OCB 使用 AES-NI 进行改进。
- 在 ARMv8/CE 上加速 AES-XTS（速度提高 2.5 倍
- 为 Blake-2 添加 AVX 和 AVX2 实现（速度提高 1.3/1.4 倍）。
- 使用 Intel SHA 扩展进行 SHA-1 和 SHA-256（速度提高 4.0/3.7 倍）。
- 使用 ARMv7/NEON 加速 GCM 实现（速度提高 3 倍）。
- 使用 i386/SSSE3 加速 SHA-512（在 Ryzen 7 上速度提高 4.5 倍）。
- 使用 64 位 ARMv8/CE PMULL 进行 CRC（速度提高 7 倍）。
- 提高 CAST5 的性能（速度提高 40% 到 70%）。
- 提高 Blowfish 的性能（速度提高 60% 到 80%）。
- 在调试助手工具中检测除法溢出
- 使用恒定时间 mpi_inv 和相关变更。
- 通过 clock_gettime 收集额外的熵。请注意，在任何体面的硬件上，不使用此回退代码路径。
- 通过 gcry_mpi_print 支持不透明 MPI。
- 为 RFC-8410 添加 Ed25519 和 Curve25519 的 OID 别名。
- 支持某些曲线的压缩格式中读取 EC 点。
- 接口变更：

gcry_mpi_get_ui	新增函数。
GCRYCTL_AUTO_EXPAND_SECMEM	新增控制代码。
gcry_sexp_extract_param	扩展。
GCRY_CIPHER_GOST28147_MESH	新增密码算法。
GCRY_CIPHER_SM4	新增密码算法。

GCRY_CIPHER_MODE_EAX	新增模式。
GCRY_ECC_CURVE25519	新增曲线标识。
GCRY_ECC_CURVE448	新增曲线标识。
gcry_ecc_get_algo_keylen	新增函数。
gcry_ecc_mul_point	新增函数。
GCRY_MD_SM3	新增哈希算法。
GCRY_MD_SHA512_256	新增哈希算法。
GCRY_MD_SHA512_224	新增哈希算法。
GCRY_MAC_GOST28147_IMIT	新增消息认证码算法。
GCRY_MAC_HMAC_GOSTR3411_CP	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2B_512	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2B_384	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2B_256	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2B_160	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2S_256	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2S_224	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2S_160	新增消息认证码算法。
GCRY_MAC_HMAC_BLAKE2S_128	新增消息认证码算法。
GCRY_MAC_HMAC_SM3	新增消息认证码算法。
GCRY_MAC_HMAC_SHA512_256	新增消息认证码算法。
GCRY_MAC_HMAC_SHA512_224	新增消息认证码算法。
GCRY_MAC_CMAC_SM4	新增消息认证码算法。

5.7.143. libgtop2：

- 移除二进制文件的 rpath 属性

5.7.144. libldb：

- 删除二进制文件的 rpath 属性

5.7.145. libmbim：

- 删除二进制中的 path 属性

5.7.146. libmetalink：

- 安全编译选项启用 fPIE，可执行命令移除 rpath

5.7.147. libmtp：

- 增加多个设备支持
- 支持 qume mtp 虚拟化设备
- 支持大于 4GB 文件处理

5.7.148. libpcap：

- 新增以下函数用于捕获 dpdk 网络包：pcap_dpdk_dispatch、pcap_dpdk_findalldevs、pcap_dpdk_create
- 新增 rpcap-over-TLS、DLT_LINUX_SLL2、ICMPv6（令牌）、DSA 数据等协议的支持；
- 增加 pcap_init()用于初始化全局设置；
- 删除对 SITA 的支持（未使用）；
- 不再支持旧版本的 libnl 编译；

5.7.149. libpfm：

- 新增更多可支持的 cpu 型号;

- patch 修改新增海光 cpu pmu 性能事件支持；

5.7.150. libpsl：

- 去除二进制文件中的 rpath 属性，提升安全

5.7.151. libpwquality：

- difok 参数指定了在新密码中允许与旧密码相同的字符数的上限，以前是 1，改成默认是 5;

5.7.152. librabbitmq：

- 修改说明文件 README.md 中默认 build 的错误描述；
- OpenSSL 应忽略已丢失的配置文件；

5.7.153. librsvg2：

- 增加 lonngarch64 架构支持

5.7.154. libseccomp：

- 主包去掉了对 help 包的弱依赖

5.7.155. libselinux：

- 更新依赖 libsepol 版本为 3.1

5.7.156. libsepol：

- 添加多处 oom 检查；
- 避免 context_struct_compute_av() optional 上潜在的 NULL 解引用；
- 检查内存被分配给的实际指针，而不是它的父数组指针

5.7.157. libspectre：

- 完善打印显示功能

5.7.158. libssh：

- 在使用 strtoul 调用时添加 errno。

5.7.159. libstoragemgmt：

- 优化了 fs resize 变化小于 1 block size 时处理

5.7.160. libtasn1：

- 为不推荐的宏打印不推荐消息。
- 恢复 SIZE 节点的处理。
- 对用 malloc 分配的内存在使用之前没有做有效检查。

5.7.161. libtimezonemap：

- 时区地图去掉国家的边界

5.7.162. libtirpc：

- 在 libtirpc 中用数组替换链表

5.7.163. libusb：

- 添加子包 libusb-tests-examples

5.7.164. libvncserver：

- 对 CMake 构建系统进行了小调整；
- 大量文档更新和标记；
- LibVNCClient 和 LibVNCServer 使用的独立加密例程被重构为两个库通用的实现;
- 在 libvncclient 模块中增加了连接超时和读取超时支持；
- 支持 OpenSSL1.1.x;添加了对 X509 服务器证书验证的支持等功能

5.7.165. libXv：

- 默认打开 --disable-static 选项，不生成静态库

5.7.166. lightdm：

- 删除对 pam_console.so 的依赖

5.7.167. linux-sgx：

- 安装依赖增加 glibc>=2.28-66
- postun 区分卸载和升级：卸载的时候删除相关配置及服务、 升级的时候保留配置及 service 文件

5.7.168. lldpad：

- 优化检查设备的有效性

5.7.169. llvm：

- 移除可执行文件的 rpath/runpath 属性值、提升安全；

5.7.170. log4j：

- 在 Interpolator 中更正 SpringLookup 包名称。
- 不带前缀的查找仅按预期从配置属性读取值。
- log4j-to-slf4j 将提供的 MessageFactory 考虑在内。
- log4j-to-slf4j 不再重新插入格式化的消息内容。
- 请求位置时，ExtendedLoggerWrapper.logMessage 不再重复日志记录。
- 要求指定 log4j2.Script.enableLanguages 以启用特定语言的脚本。
- 将 log4j 添加到 jul JDK 日志
- 默认情况下，通过 url 将配置加载限制为 https
- 将 TB 支持添加到 FileSize
- 为属性配置格式添加简写语法，用于指定记录器级别和 appender-refs

- 如果 LoggerFactory 作为属性提供，则将 LogManager 标记为已初始化。
- 修改 pom.xml 所需 jar 版本，

5.7.171. lorax：

- aarch64：在 initrd.img 中添加 ngbevf txgbevf rnpvf rpngbevf grtnic mwv207 ljmcore vrcdrv 驱动程序
- x86_64：在 initrd.img 中添加 ngbevf txgbevf rnpvf rpngbevf grtnic l jmcore vrcdrv 驱动程序
- loongarch64：在 initrd.img 中添加 ngbevf txgbevf rnpvf rpngbevf gr tnic vrcdrv 驱动程序。
- 在 initrd.img 中添加 SSSRAID 驱动程序。
- 内核添加 inspur-drm sssnic 和 gb 驱动程序。
- 在 initrd.img 中添加 mlx5_core rnp rnpm nce m1600 驱动程序。
- 为 loongarch64 添加驱动程序 inspur-drm。
- 为 aarch64/86_64 添加驱动程序 inspur-drm。

5.7.172. lsscsi：

- 改进 NVMe 设备解析（例如/dev/nvme0c1n2），使得 NVMe 的 WWN 打印更加持续。
- 打印可用于 SCSI 主机的 nr_hw_queues；删除带有-HL 的 NVMe 设备名称后的空行。
- 选择要输出的最佳 SCSI id（--SCSI_id）的逻辑。

5.7.173. luajit：

- 增加 SP 安全编译选项

5.7.174. lvm2：

- 增加对 intel vroc 设备的支持
- 增加 lvmlockd 增加对 loongarch 架构的支持；

5.7.175. lxc：

- on_error 处理增加逻辑，仅初始化 lock 失败时打印
- 优化旧逻辑，使用__do_free，避免释放内存错误
- 重构 selinux 标签的转换为共享模式
- 使用"__do_free "宏，而不是调用 "free "宏，以消除对内存泄漏的担忧
- 略增加 runtime_sock 目录的权限，提升为 0700
- HAVE_ISULAD 中增加 no_controller 判断，对于没有 controller 的 cgroup 不在 payload，采用 attach 方案
- 增加场景考虑，过滤 args 为空和未提供 roofs 路径情况
- 变动策略为在 parent mounted 后建立 rootfs masked 路径
- 非 hierarchies 跳过 kill group 进程逻辑
- 增加 sw64 架构支持。
- 增加 lxc-attach 和 add-gids 选项

- 改正 lxc-attach --help 中输出，从 suffi 变更为 suffix
- 增加 loongarch64 架构支持
- 编译增加 yajl 支持。
- 在 getenv 后使用 ocihook

5.7.176. mailman：

- 优化 mailman.po 翻译内容

5.7.177. mariadb：

- INFORMATION_SCHEMA 增加了 CHECK_CONSTRAINTS 表；
- 添加新的系统变量 eq_range_index_dive_limit 来加速带 IN 的嵌套查询，为了向后兼容，默认值为 0 即表示 unlimited；
- Mariabackup 不允许使用 TRUNCATE；
- ALTER TABLE...page_compression_level 不应重建表；
- Galera library 更新至 25.3.24 ；
- mysqldump 由 utf8 改为使用 utf8mb4 作为默认字符集；
- sql_safe_updates 可以作为命令行和 my.cnf 选项；
- 减少了 INSERT...ON DUPLICATE KEY UPDATE 死锁情况；
- FOREIGN KEY 检查期间 KILL QUERY 不再导致 hang 住；
- ALTER DATABASE 在只读模式是可能的；
- slave_ddl_exec_mode=IDEMPOTENT 不处理 DROP DATABASE；

- ALTER 被打断后的孤儿临时文件导致的错误码 17 和 71 错误；
- SPATIAL INDEX 锁错误；
- MariadB 服务器和备份的几个改进，用于处理加密或 page_compressed 页面
- Galera library 更新至 25.3.25；
- HeidiSQL 更新至 9.5；
- table_definition_cache 最大值变为 2097152；
- COM_RESET_CONNECTION 更改连接编码；
- Galera library 更新至 25.3.26；
- Encryption：innodb_encrypt_tables 在 innodb_encryption_rotate_key_age=0 时也工作；
- Protocol：BULK with replace 在 account 中不使用第一个参数；
- PAM 认证模块添加选项支持用户名大小写匹配
- HeidiSQL 升级至 10.2；
- connect 升级至 1.06.0010；
- Galera wsrep library 更新至 25.3.28；
- Privileges：SHOW PRIVILEGES 现在正确列出了删除历史特权，而不是将其显示为删除版本行；
- wsrep library 更新到 25.3.29
- Variables：将 innodb_encryption_threads 值限制为 255、max_sort_length 最小值升至 8；
- Docker 添加 replication；

- 从 MariaDB10.3.8 或 10.3.9 进行升级时需要先运行 mysql_upgrade；

5.7.178. mate-desktop：

- 更新“关于银河麒麟”中的 copyright 信息到 2024 年

5.7.179. mate-indicators：

- 添加缺失的繁体中文翻译

5.7.180. mate-panel：

- 增加繁体翻译
- 修改为非 root 用户下，任务栏右键中不存在系统监视器选项

5.7.181. mate-polkit：

- 增加繁体翻译

5.7.182. mate-session-manager：

- 增加繁体翻译

5.7.183. mate-settings-daemon：

- 增加繁体翻译

5.7.184. mate-system-monitor：

- 增加繁体翻译

5.7.185. mate-terminal：

- 增加繁体翻译

5.7.186. mate-user-admin：

- 繁体修改

5.7.187. mcelog：

- 更改 i10nm 平台 DDR4 字符串为 DDR，不区分 DDR4 与 DDR5；

5.7.188. mcpp：

- 一些敏感词的修改

5.7.189. mdadm：

- mdcheck_start.service 和 mdcheck_continue.service 服务配置中启动命令文件不存在。
- cifs 用例执行完后产生 core 日志。
- mdmonitor-oneshot.service 服务启动失败。
- 当无 raid 时，可以正常启动 monitor 。
- Dump:还原元数据时从错误的元数据文件获取 stat。
- 阻止创建大小小于 1M 或区块的 IMSM 卷。
- 组装：用故障的“best”设备防止 segfault

- IMSM：将“validate_container_IMSM”移动到 mdassembly 中
- DDF：将数据偏移量信息添加到--检查输出。
- Monitor：有时以只读状态写入元数据。

5.7.190. mod_wsgi：

- 打包新增配置文件 wsgi-python3.conf

5.7.191. mokutil：

命令选项部分新增--ca-check、--ignore-keyring，删除--simple-hash，

新增加 CA 检查及 kernel keyring 检查功能；

引入了 SBAT 支持吊销更新功能，这个功能会在 shim-15.6 中可能被使用到；

5.7.192. mtools：

- 如果我们执行只读访问，则忽略图像文件锁定错误。
- 支持重新映射数据。
- 修改 mpartition 中的一致性检查。
- 设备大小处理重构。
- 允许 remap 写入零备份扇区。
- fs_init 失败时所有失败案例的错误消息。
- 删除在放弃对仍在其他地方引用的流节点的引用时触发的无用缓冲区刷新。
- 在 mformat 中，使 Fs 动态分配，而不是在堆栈上，以便能够使用 stream.c 提供的实用程序
- 防止试图创建零大小的缓冲区。

- OptionConverter 可能导致 StackOverflow 错误。
- 在 XDF_IO 中，即使 FDC 以前处于错误状态，也要重试足够的次数才能真正成功
- 配置脚本和大文件处理的总体简化
- 在 lseek 使用 32 位偏移的情况下，更喜欢 lseek64 而不是 llseek

5.7.193. nagios：

- 使用 systemd 时，将在重新加载之前验证配置；
- 重新加载 Nagios 创建失效的进程；
- 默认配置在 nagios 中激活了查询处理程序，有一个 perl 程序，打开一个 socker，注册查询处理程序和停止，在对它执行 strace 操作报错；

5.7.194. nano：

- 优化部分参数，
- 优化文档缓冲，
- 优化部分语法高亮
- 优化缩进功能，
- 优化 rc 文档大小写
- 新增--wordchars 单词计数，优化缓冲区使用，优化快捷操作及消息提示
- /etc/nanorc 中新增三个配置项

5.7.195. ncompress：

- 新增-h 命令参数，打印帮助信息

5.7.196. ncurses：

- 新增 loongarch64 架构支持；

5.7.197. ndctl：

- 执行 ndctl destroy-namespace -f all 命令时跳过大小为 0 的命名空间，以避免异常

5.7.198. neon：

- 优化代码，使用 destroy_and_wait()替换 test/*.c 文件中接口的退出逻辑；
- GX 已经弃用，修改 neon.mak 文件，使用 EHsc 替换掉 GX；
- 定义适当的宏，减少编译过程中的 warning 信息；

5.7.199. net-snmp：

- 添加 aes192 & aes256 支持

5.7.200. nettle：

- 新增支持 SM2 、SM3 国密算法

5.7.201. net-tools：

- 将 pointopoint 短标志从 P 更改为 p

5.7.202. netty：

- 增加编译选项 strip

5.7.203. network-manager-applet：

- 网络主机名配置界面部分英文未繁体转化和二次补充繁体化翻译。
- 网络连接添加网络等界面存在英文
- 查看网络连接信息 关闭按钮未繁体中文转化
- 右下角右击电脑图标点 关于存在英文
- 网络编辑界面存在英文
- 时间与日志配置中地区和城市名称显示异常

5.7.204. nfs-utils：

- nfs-utils 新增 gss-proxy 功能，提供了一种代理机制，用于在客户端和服务端之间进行 GSS-API 身份验证的代理。

5.7.205. nftables：

- 安全编译选项启用 fPIE，可执行命令移除 rpath

5.7.206. nghttp2：

- 执行 nghttpd 8080 --no-tls -v -n -1，出现 core dumped：将 strtoul 和 strol 替换为 parse_uint；

5.7.207. nginx：

- limit_rate 和 limit_rate_after 指令增加变量支持；
- stream 模块中增加 proxy_upload_rate 和 proxy_download_rate 指令的变量支持；
- 增加 limit_req_dry_run 指令；在 upstream 块中使用 hash 指令时，空 hashkey 现在会触发 round-robin 平衡；
- gzip 使用 zlib 来写入头尾；
- $r->internal_redirect()嵌入的 perl 方法现在期望转义的 URIs；
- $r->internal_redirect()perl 方法支持命名位置；
- 优化对 HTTP/2 的处理；
- 优先使用 ioctl，避免瞬时连接消耗太多时间；
- 支持$proxy_protocol_server_addr 和$proxy_protocol_server_port 变量；
- 支持 limit_conn_dry_run 指令；
- 支持$limit_req_status 和$limit_conn_status 变量；
- grpc_pass 指令支持变量；
- 不允许多个“Host”请求头行；
- 支持 directive 指令
- 使用 OSCP 进行客户端证书验证；
- lingering_close、lingering_time、lingering_timeout 指令在 HTTP/2 下进行使用；
- 后端发送的额外数据总是被丢弃；
- 收到来自 gRPC 后端长度不正确的响应 Nginx 会进行报错；

- 支持 proxy_cache_path、fastcgi_cache_path、scgi_cache_path、uwsgi_cache_path 指令的 min_free 参数；
- 在可用的 worker 连接耗尽之前，nginx 开始关闭 keepalive 连接并对此在错误日志中记录 warning 信息；
- 使用分段传输编码时优化客户端请求读取；
- 增加 ngx_stream_set_module 模块；
- 增加 proxy_cookie_flags 和 userid_flags 指令）
- 支持 ssl_conf_command、proxy_ssl_conf_command、grpc_ssl_conf_command、uwsgi_ssl_conf_command、ssl_reject_handshake、proxy_smtp_auth 指令；
- 增加-e 开关，可用来设置日志错误日志路径；现在构建插件模块时可以在不同的模块中指定相同的源文件；
- 在请求主体中过滤内部 API；
- keepalive_timeout 和 keepalive_requests 指令替换 http2_recv_timeout、http2_idle_timeout、http2_max_requests 以更好的兼容 HTTP/1.X；
- large_client_header_buffers 指令用于替代 http2_max_field_size 和 http2_max_header_size 指令；
- 现在如果空闲的 worker 连接耗尽，nginx 不仅开始关闭 keepalive 连接，同时也包括了 lingering_close 即延迟关闭的连接；
- proxy_cookie_flags 指令增加变量支持；
- mail 代理中 listen、proxy_protocol、set_real_ip_from 指令支持 proxy_protocol 参数；

- keepalive_requests 指令的默认值改成 1000；
- 增加 keepalive_time 指令；
- 增加$connection_time 变量
- 兼容 OpenSSL 3.0；
- 增加了 max_errors 指令的支持；
- proxy_ssl_certificate、proxy_ssl_certificate_key、grpc_ssl_certificate、grpc_ssl_certificate_key、uwsgi_ssl_certificate、uwsgi_ssl_certificate_key 支持变量；
- 对 CONNECT 方法总是返回一个 error；
- 如果请求中同时包含 Content-Length 和 Transfer-Encoding 头行会返回错误；
- 如果请求行出现空字符，返回错误；
- 如果 header 名称出现空字符，返回错误；
- 当使用多个监听 socket 时优化配置测试；
- 当超过 64 个 buffer 时，减少了 long-lived 请求的内存消耗
- 拒绝 Transfer-Encoding 头的 HTTP/1.0 请求；
- 不再支持导出密文；
- 兼容 openSSL 3.0；
- Auth-SSL-Protocol 和 Auth-SSL-Cipher 头行现在传递给邮件代理认证服务
- 请求过滤 API 允许数据缓存处理
- 对使用 HTTP/2 时对客户端请求读取进行优化；

- 在请求主体中过滤内部 API；
- 使用 NPN 替代 ALPN 用于建立 HTTP/2 连接；
- 拒绝 ALPN 的 SSL 连接；
- sendfile_max_chunk 指令默认值变更为 2；
- 增加 proxy_half_close 指令、ssl_alpn 指令、$ssl_alpn_protocolvi 变量的支持；
- 使用 OpenSSL3.0 时支持 SSL_sendfile()；
- ngx_http_mp4_module 模块中支持 mp4_start_key_frame 指令；
- 收到长度不正确的代理响应时 nginx 可能会缓存连接；
- 不合法的后端 header 记录成 loginfo 级别取代 error 级别；
- nginxm 改为默认使用 PCRE2 库进行构建；
- nginx 在 freeBSD 上总是使用 sendfile(SF_NODISKIO)；
- 支持$ssl_curve 变量；

5.7.208. nss-altfiles：

- 新增/etc/protocols，/etc/rpc，/etc/hosts，/etc/networks，/etc/services，/etc/shadow，/etc/gshadow 等文件信息的读取

5.7.209. nss：

- nss 及 nss-util 不在依赖 nss-help 包

5.7.210. ntp：

- 当 ntpd 删除最后一个接口时，增加检查防止 NULL 指针 deref 崩溃
- 通过安装后处理脚本增加 sntp 服务状态保障；

5.7.211. numad：

- 新增帮助文档

5.7.212. nvme-cli：

- NVMe 字符设备功能加入了两个 RPC 命令 bdev_nvme_cuse_register 与 bdev_nvme_cuse_unregister。它们分别用于指定为某 NVMe 设备创建 CUSE 字符设备，和注销 CUSE 字符设备。

5.7.213. nvmetcli：

- 清理时不要删除 ANA 1 组；
- 修改 README 中关于 configshell-fb 的链接地址；
- 优化还原时的 IOError 处理；
- 移除冗余的显式关闭函数 close()；
- 使 modprobe 也适用于 kmod lib；
- 允许不同的设备进行测试；
- 新增一个 tcp 示例的 json 文件；
- 新增 tcp.json 配置文件，作为 tcp 类型配置文件 demo 模板
- 新增接口：_get_grpid()、_list_ana_groups()、ngiud_set()、summary()、

ui_command_grpid()、UIPortNode.summary()、ls()

- 移除接口：status()

5.7.214. ocaml：

- 新增-fPIC 编译选项用于生成位置无关代码。
- 对 loongarch 和 mips 进行特殊处理，禁止编译以及验证 opt 相关工具

5.7.215. opencl-headers：

- 新增头文件：cl_half.h、cl_icd.h

5.7.216. open-isns：

- isnsadm 命令新增-V 和-r 参数支持
- 默认启用 IPv6 socket 监听

5.7.217. openjpa：

- 移除 openjpa 对于 httpunit 的依赖
- 修改协议信息

5.7.218. openmpi：

- 修改/usr/lib64/openmpi/bin 路径为/usr/bin

5.7.219. openscap：

- 移除可执行文件的 rpath/runpath 属性值

5.7.220. openssh：

- 新增支持 sm3-hmac 国密算法选项；
- 优化升级 ssh 远程连接加密算法模式；

5.7.221. os-maven-plugin：

- 添加 LoongArch 架构支持

5.7.222. paho-c：

- 新增 ipv6 本地监听端口可配功能

5.7.223. passwd：

- 优化繁体中文支持

5.7.224. pcp：

- 增加 pcp 领域的 selinux 策略。

5.7.225. pcre2：

- 避免返回部分匹配，使结果与 JIT 一致；

- 支持 loongarch 架构
- 支持申威架构

5.7.226. perl-Carp_Clan：

- 去掉对 perl 版本低于 5.005 的语法兼容以提升程序执行效率

5.7.227. perl-Config-AutoConf：

- 增加 extra_link_flags 可选入参用于 search_libs 函数，
- 增加.perltidyrc 文件

5.7.228. perl-Crypt-CBC：

- 分离出 help 子包

5.7.229. perl-Crypt-DES：

- 新增 help 子包

5.7.230. perl-Crypt-OpenSSL-Guess：

- 在执行 brew --prefix 时使用--installed 选项
- 增加 help 子包

5.7.231. perl-Data-Dump：

- 使用 Data::Dump::LINEWIDTH 参数代替硬编码的 60

5.7.232. perl-Data-OptList：

- 增加 docs 文档中支持 perl 版本说明
- 去掉 goto 实现以提升执行速度

5.7.233. perl-Data-UUID：

- fopen 打开文件前设置文件 umask
- 使用 File::Spec 获取 tmpdir 以代替硬编码

5.7.234. perl-Date-Manip：

- 时区信息更新
- 调整 tzdata 文件检查优先级以处理 docker 场景问题

5.7.235. perl-Devel-CheckLib：

- 使用 Capture::Tiny 代替 Capture::Output 方法
- 重构测试代码,去掉 gcc 优化

5.7.236. perl-Encode-Locale：

- 定义 mod_name 以对规范文件进行操作

5.7.237. perl-Encode：

- 增加栈保护编译选项，防止溢出问题

5.7.238. perl-File-Listing：

- 修改 apache 默认索引，忽略确知的 apache 索引导航链接

5.7.239. perl-Getopt-Long：

- 添加了回调对象中的'given'方法。该方法返回用户传递的选项名称

5.7.240. perl-HTTP-Message：

- 处理 LWP::UserAgent 响应重定向处理程序的特定响应标头中出现“uninitialized value”
- 配置文件添加 backcompat 常量和 425 响应状态码描述；
- 清理存在重复的 backcompat 常量；
- 将响应码 308（永久重定向）添加到 is_cacheable_by_default 定义中；
- 在 HTTP::Status 中移除 Exporter 的继承 2 和 3 的链接；
- 允许“can”方法响应委托的方法；
- 捕获 headers 中空值、空名称问题；

5.7.241. perl-IO-HTML：

- 新增了使用示例文件 detect-encoding.pl

- 增加$bytes_to_check 变量配置的对应 test 用例，字符串没以右引号结尾的改为 return 中止程序
- 增加 $bytes_to_check 变量配置，原来写死 1024，现在默认 1024 可配

5.7.242. perl-IPC-SysV：

- 在 SysV.xs 文件中，存在有符号的整数和无符号整数间的比较

5.7.243. perl-libwww-perl：

- 支持文件句柄作为输入的下载
- 使用 File::Copy::move 方法尝试自动备份持久化
- 更新 docs 文档中协议允许与协议禁止部分内容
- 增强了 LWP::UserAgent 中的哈希串生成随机性

5.7.244. perl-LWP-Protocol-https：

- test 用例优化，引入 Net::SSLeay 模块
- 修改支持链接中使用的 SSL/TLS 协议版本获取
- 更新 Mozilla::CA 依赖

5.7.245. perl-Module-Build：

- 更新配置编译测试的先验依赖，用 COMPARISON 代替 MOTIVATIONS
- 优化 pureperl-only 特性支持

5.7.246. perl-Module-ScanDeps：

- 优化 PerlIO 方法的匹配调用，XML::Twig::XPath 的依赖模块等
- 改进路径以/结尾的方式，更多的使用 use lib
- FindBin 等方法的引用方式优化
- 增强_find_encoding()方法实现

5.7.247. perl-MRO-Compat：

- 优化 perl5.8 上纯 perl 实现的 DFS(深度优先搜索)继承算法

5.7.248. perl-Net-HTTP：

- 完善对 PeerAddr 地址为 0 的处理功能

5.7.249. perl-Net-LibIDN2：

- 支持 IDN2_NO_TR46 和 IDN2_NO_ALABEL_ROUNDTRIP
- 添加精确的 perl 错误码
- 测试程序增加 TR_46
- 将文档调整到当前支持的 libidn 级别

5.7.250. perl-Path-Tiny：

- 新增 size 和 size_human 方法，支持类似 ls -lh 方式的文件大小显示输出

- 优化 tempdir 和 tempfile 方法更好的区别文件和路径的处理

5.7.251. perl-Pod-Escapes：

- 加固标准化测试，删除无关输出

5.7.252. perl-Pod-Markdown：

- 作为 pm 模块使用时增加 escape_url 可选参数可初始化关闭（默认开启）
- local_module_url_prefix 可赋值为”

5.7.253. perl-Socket6：

- 更新 test 用例

5.7.254. perl-Software-License：

- 增加 program 参数更好的支持 license 文本内容处理
- 更新 Artistic License 1.0，Apache 2.0，CC0 等许可协议内容
- 增加 SPDX license 表述支持

5.7.255. perl-Sub-Name：

- 优化 Sub::Util 类内部实现
- 重命名 lexical 函数方法，适应于 perl 5.22 以上版本
- 优化 DB::sub 更好的适应宽字符和 null

5.7.256. perl-Thread-Queue：

- 定义 mod_name 以对规范文件进行操作

5.7.257. perl-TimeDate：

- 去除 Date::Parse 中"Time::Local”导致的限制

5.7.258. perl：

- ldd 命令查看 perl 动态库文件依赖报大量“undefined symbol”错误，分析确认问题原因为软件包中 re.so 等动态库未主动链接-lperl

5.7.259. perl-Types-Serialiser：

- 新增 Types::Serialiser::as_bool 方法，该方法是 Types::Serialiser 模块中提供的一个函数，其作用是将给定的值转换为布尔值

5.7.260. perl-Unicode-Collate：

- DUCET 文件的更新到 13.0.0
- UCA_Version 更新到 43

5.7.261. pesign：

- 新增 elfsign 命令行工具，执行对 elf 文件进行签名和验证

- 优化功能，如果找不到证书，则提供免费资源。
- 添加支持 sm2、sm3 算法

5.7.262. php：

- PHP 应用程序解析 cookie 异常问题：网络和同站攻击者能够在受害者的浏览器中设置一个标准的不安全的 cookie

5.7.263. pluma：

- 增加繁体翻译

5.7.264. policycoreutils：

- 添加 ExecStartPost 选项到 rerecond.service
- os.makedirs 使用 exist_ok=True 参数作为判断。
- 发生错误时调用 fclose(fp)关闭文件流
- 将删除命令与其他命令分开，以便它们可以在单独的事务中应用
- 如果 fcontext 不是本地数据库，就不再查询。
- 在 load_checks()中，增加对 malloc()的返回检查，以避免 NULL 引用

5.7.265. postfix：

- postfix 安装后 postfix.pem 证书有效期小于 1 年
- 移除二进制文件的 runpath 设置

5.7.266. ppp：

- 在部分函数中，文件指针使用后存在未进行 fclose 操作释放资源

5.7.267. proftpd：

- 支持 SOURCE_DATE_EPOCH 环境变量，用于可复制的构建
- 实现对使用 SSL/TLS 为 LDAP 连接配置证书选项的支持
- 以非 root 用户身份运行时忽略补充组
- 在可用的情况下使用时间函数的可重入版本
- mod_sftp 现在支持 Ed25519 密钥
- mod_sftp 现在支持 RSA SHA-2 公钥签名
- 默认启用 RootRevoke
- mod_tls 模块现在在启动时对配置的 tls 文件执行基本健全性检查
- 当使用 TLS 时，mod_deflate 模块支持 MODE Z 数据传输
- mod_xfer 模块现在支持 RANG FTP 命令
- ftpasswd 脚本支持从组中删除用户
- 重构了 LogFormat 处理代码，使其不再冗长
- 为 mod_sftp、mod_tls 生成新的 DH 参数

5.7.268. pulseaudio：

- 移除可执行文件的 rpath/runpath 属性值、提升安全

5.7.269. pyflakes：

- 移除不再使用的 tracing 用法，
- 为 checker 模块新增 MATCH 描述支持
- 在使用 from future import annotations 时更好地支持仅注解的赋值使用
- 识别 TypeVar 的特殊情况类型
- 在 all 中显示未定义的导出的错误，按确定顺序显示
- 在错误消息中包含列信息
- 添加对赋值表达式（PEP 572）的支持
- 新增 yaml 文件：pyflakes.yaml

5.7.270. pyScss：

- 取消对 python 3.2 的支持；
- 增加对 CSS shape 函数的支持；
- 修改 zip 元信息,将 setup 函数中 zip_safe 参数指定为 False
- 使 C 扩展可选；

5.7.271. python3：

- 禁用了 x86 和 i386 架构的 optimizations。
- 使测试套件支持上游 Expat>=2.4.5
- VE-2022-45061
- 不要显式调用 PyThread_exit_thread（）

- 新增 loongarch 架构支持。

5.7.272. python-alsa：

- 删除了冗余 provides：python-webob

5.7.273. python-attrs：

- attr.s() 新增 field_transformerhook，它会对所有的属性进行调用，并返回一个（已修改或已更新）的属性实例列表。
- attr.asdict()新增 value_serializer hook，可以改变值的转换方式。这两个 hook 都旨在帮助数据（去）序列化工作流。
- kw_only=True 现在在 Python 2 上也能工作。
- raise from 现在在 PyPy 的 frozen 类上也能工作。
- attr.asdict() 和 attr.astuple() 现在在处理 retain_collection_types 参数时将 frozensets 当作 set 处理。
- attr.s() 和 attr.make_class() 的类型存根不再缺少 collect_by_mro 参数。
- attr.define() et al 现在能够正确检测到 eq 和 ne。
- attr.define() et al 的混合行为现在也能够正确处理参数传递。
- 在有插槽的类上，可以再次定义自定义的 setattr 方法。
- 在 20.1.0 版本中，我们在 attr.Attribute 类上引入了继承属性，以区分继承的属性和直接在类上定义的属性。然而，当比较 attr.Attribute 的实例时，涉及该属性会导致问题，因为在子类化时，基类的属性突然之间与超类中的属性不相等。因此，现在比较 attr.Attribute 的实例时将忽略继承属性。

- 如果运行测试套件时未安装 zope.interface，与接口相关的测试将自动跳过。
- 使用 @define(frozen=True)创建冻结类和继承冻结类的体验已经得到改进：不再需要设置 on_setattr=None。
- 增加了 attr.resolve_types()。它确保所有前向引用和字符串形式的类型都被解析为具体类型。只有在运行时需要具体类型时才需要此功能。这意味着，如果您只使用类型进行静态类型检查，则不需要此函数。
- 新增 attrs 自动生成 pickling 所需的对有插槽的类进行序列化的 setstate 和 getstate 方法。
- 添加了 attr.converters.pipe()功能。该功能允许通过管道将所有值传递给多个转换回调组合成一个，并返回最后一个值。
- @attr.s(auto_exc=True) 现在生成按 ID 进行哈希的类，如文档中始终声明的那样。
- 添加 attr.validators.matches_re()，用于检查字符串属性是否匹配正则表达式。
- 已添加 attr.version_info，可用于可靠地检查 attrs 的版本并编写向前和向后兼容的代码。
- 增加了 is_callable、deep_iterable 和 deep_mapping 验证器。
- attrs 现在自带 PEP 484 类型提示。与 mypy 的 attrs 插件结合使用，支持 Python 2 和 Python 3 中编写静态类型的代码
- 添加了关于 attrs 中类型注解的叙述性文档。
- 向 attr.ib 和 attr.s 添加了 kw_only 参数，并向 attr.Attribute 添加了相应的 kw_only 属性。这一变化使得在 Python 3 上生成带关键字参数的 init 方法成为可能，从而放宽了对默认值和非默认值属性的顺序要求。

- attr.asdict() 现在可以正确处理深层嵌套的列表和字典。
- 添加了 attr.converters.default_if_none()，允许替换属性中的 None 值。例如，attr.ib(converter=default_if_none("")) 将 None 替换为空字符串。
- 现在可以通过传递 @attr.s(weakref_slot=True) 使具有插槽的类成为弱引用的。
- 向 @attr.s 添加了 cache_hash 选项，该选项会导致对象的哈希码只计算一次并存储在对象上。
- 新增支持属性可以命名为 property 和 itemgetter。
- 现在可以通过类注解覆盖基类的类变量。
- x=X(); x.cycle = x; repr(x) 将不再引发 RecursionError，而是显示为 X(x=...)。
- attr.ib(factory=f) 现在是对常见情况 attr.ib(default=attr.Factory(f))的语法糖。
- 添加了 attr.field_dict()，用于返回一个有序字典，其中包含一个类的 attrs 属性，键为属性名称。
- 在带有插槽的类中，getstate 和 setstate 现在忽略了 weakref 属性。
- 如果向 attr.s 传递了一个 theses 参数，它将不再尝试从类体中删除具有相同名称的属性。
- attr.NOTHING 的哈希现在是纯素且在 32 位 Python 构建上更快。
- 实例化冻结的字典类所涉及的开销几乎被消除。
- 生成的 init 方法现在具有一个从字段类型派生的 annotations 属性。
- 重新整理了文档，以反映 attrs 的范围增长。我们没有将所有内容都放在示例页面上，而是开始提取叙述章节。添加了初始化章和哈希章。

5.7.274. python-blivet：

- 新增支持 udf-filesystem 文件系统
- 新增支持 loongarch64 架构
- 新增支持 sw64 架构
- 从 PartitionFactory 中排除不可用的磁盘
- 适应 dosfstools 4.2 FAT 标签更改
- 将 liblockdev 版本升级到 2.24
- 新增对创建 LVM VDO 池和 LVM VDO 卷的支持
- 增加了为 LUKS 2 设备指定扇区大小的支持
- 取消限制 swap 分区到 128 GiB
- 添加基本的 F2FS 支持
- 使 safe_device_name 指定设备类型
- 将 exFAT 添加到可识别的文件系统
- 在只读模式下使用 xfs_db 获取 XFS 信息
- 忽略 vmbackkedtestcase 中的 zRAM 设备
- 添加对 XFS 格式增长的支持
- 忽略在 sysfs 中标记为隐藏的设备
- 不忽略未知/不支持的设备映射器设备
- 允许为 LUKS 2 格式指定自定义哈希函数
- 为 LVM VDO 添加可用性函数

- 在填充期间将 VDO 池数据 LV 添加到内部 LV
- pylint:忽略关于线程的弃用警告
- 删除 device_properties_test 中的 pdb 断点
- pylint:删除 doc/conf.py 中字符串的冗余'u'前缀
- pylint:忽略 i18 .py 中的" redundancy -u-string-prefix"警告
- pylint:忽略新的警告 W1514 "unspecified-encoding"
- Makefile:为 potfile 目标指定 webblate 存储库分支
- 允许为 UnavailableMethod 指定自定义错误消息
- 在 setup.py 中使用 setuptools 而不是 distutils
- 忽略 pylint 参数- do_tasks 的差异警告
- 从 LUKS_Data 中删除未使用的__save_passphrase 成员
- 忽略新的 pylint 警告"arguments-renamed"
- 不要使用 deprecated
- 从 DeviceFactory 中删除未使用的成员__names
- 改进缺少依赖项打印的错误消息
- 不要为 RAID 1 设置块大小
- 确保在运行 pvcreate 之前更新了 LVM 配置
- LVM 暂时忽略新设备文件
- 将 LVM 筛选器列表转换为集合
- 从 LVM 拒绝列表中删除操作设备
- 在配置设备格式之前，请确保设备已经安装好
- 在依赖列表中使用包列表而不是循环

- 添加用于在 VM 中运行测试和开发的迁移文件
- 更新我们的剧本以安装测试依赖项
- 添加 LUKS 加密 LV 到 LVM 示例
- 添加 LVM 精简配置示例
- 允许在没有 Python SELinux 模块的情况下运行 blivet
- 为 LVM 扇区大小不一致添加一个特殊的异常类型
- 从 Blivet 类(vtrefny)中删除“encryption_passphrase”属性
- 为 EFIFS 分区使用 PARTITION_ESP 标志
- 为扇区大小不一致的 LVM 提供更好的错误消息
- 避免没有 DiskLabel 类型的 DiskLabel 格式出现 AttributeError 错误
- 当尝试对齐分区大小时忽略 arithmetierror
- 当尝试获取 ISCSI 启动器名称时，不记录整个异常
- 将文件操作周围的 IOError 替换为 OSError
- 规范:添加'make'到 buildrerequires
- 将目录的 SELinux 上下文应用到新创建的挂载点
- 如果 UDev 查找失败，尝试使用 libblockdev 获取 Btrfs 卷 UUID
- 允许移除不支持 VDO 的 LVM VDO 设备
- 在任务中使用更好的 libblockdev 插件
- 设置 LVM VDO 池设备的最小大小
- 在创建 VDO 逻辑卷时默认添加 nodiscard 选项
- 允许在运行 mkfs 时添加 nodiscard 选项

- 添加对 LVM VDO 设备的基本支持
- 添加 LVM VDO 设备工厂
- 允许使用“blivet”创建 LVM VDO 池和卷
- 在 blivet.flags.btrfs_compression 中应用压缩设置
- 在父分区名称更改后更新 LUKS 设备名称
- 在名称检查中，将已使用的名称添加到错误消息中
- 当使用产品名称作为设备名称时，确保产品名称安全
- 启动 iscsi-init 服务
- 对于部分隐藏的多路径设备使用 UnusableConfigurationError
- 如果读取设备失败，关闭 fd
- 在调整 thinpool 元数据大小时考虑 pmspare 的增长
- 在写入 ks 分区信息时，舍入到最接近的 MiB 值
- 添加_teardown 方法到 IntegrityDevice
- udev:添加函数来获取设备持有者列表
- 添加对 LVM 写缓存设备的基本支持
- 对于不能挂载的文件系统跳过 test_mount
- 使扩展分区可调整大小
- 增加了对设备标签的支持
- 删除 po 文件夹
- 恢复"为 EFIFS 分区使用 PARTITION_ESP 标志
- 文档更新：
- README:添加关于 openSUSE/Mageia/OpenMandriva Copr repo 的信息

- 添加 LVM VDO 文档
- 添加 LVM VDO 示例
- 术语清理
- 测试用例更新：
- 为 LVM VDO 添加虚拟机测试
- 测试:运行测试时打印版本和显示位置
- 测试:允许在 PYTHONPATH 中没有测试目录的情况下运行测试
- edd_test:根据测试文件位置定位 edd_data
- 对 blvet 拉取请求运行 Anaconda 测试
- 测试完成后删除 EDD 测试日志
- 添加 util. get_sysfs_attr 测试
- 为 RAID 设备添加 udev.device_get_name 测试
- 测试:以非 roo 身份运行时跳过 test_reset
- 测试:为某些测试修补 LVM 可用性函数
- 测试:补丁 LVM lv 调用一些非 LVM 测试
- 添加 SwapSpace 最大大小测试
- 添加 XFS 调整大小的测试

5.7.275. python-bottle：

- 移除“fast”的不再使用的实现，
- setup 新增对 python3.4~3.7 语言支持，

5.7.276. python-breathe：

- 使用 Sphinx 构建文档时偶现报错 AttributeError: 'NoneType' object has no attribute 'content_'，需要优化无类型参数处理。
- 通过将信号视为函数来增加对 QtSignals 的适当支持。
- 优化解析器异常时打印文件名
- 使用 sphinx 1.7.5
- Doxygen 文档中的换行没有正确呈现，需要将换行符显示为单独的段落。

5.7.277. python-chardet：

- python3-chardet 新增提供 python_provides

5.7.278. python-futures：

- ThreadPoolExecutor 类构造函数现在接受一个可选的' thread_name_prefix'参数，以便自定义池创建的线程的名称。
- 明确 python-future 支持 python 版本的范围。

5.7.279. python-httplib2：

- 新增 python-httplib2

5.7.280. python-httpretty：

- 修改 mock 时间，使基于时间的测试更加可靠。

- 在 URIMatcher 类的 matches 方法中参数匹配部分进行代码逻辑完善。

5.7.281. python-hypothesis：

- 弃用带有空序列的 sampled_from（ ）。
- 此更新添加了 report_multiple_bugs 设置，可以使用该设置禁用多个错误报告，并且只引发最小示例的错误。
- 使调用 float（min_value=inf，exclude_min=True）或 float（max_value =-inf，exclude_max=True）成为显式错误。float（min_value=0.0，max _value=-0.0）现在已弃用。
- 阻止了 Hypothesion 在 Python 3.4 上的安装.
- 支持将 timedelta 作为 deadline 设置
- 允许 register_type_strategy（ ）与 typing.NewType 实例一起使用。
- 添加了 broadcastable_shapes（ ）策略。
- 添加了 functions（ ）策略，该策略可用于模拟回调的“真实”函数。
- from_type（ ）策略现在支持 rang 对象（或 Python 2 上的 xrange）。
- 改进了 array_shapes（ ）策略，为基于 min_side 的 max_side 和基于 mi n_dims 的 max_dims 选择适当的默认值。
- from_type（ ）策略现在支持切片对象。
- 列表的 unique_by 参数现在接受一个可调用的元组，这样生成的列表的每个元素相对于元组中的每个可调用对象都是唯一的。
- 实现了 slices（ ）策略，以生成长度大小序列的切片。
- 弃用 GenericStateMachine，而支持 RuleBasedStateMachine。

- 弃用并禁用 buffer_size 设置，该设置本应一直被视为私有实现细节。
- 显著提高了绘制元素取自 sampled_from（）策略的唯一集合的性能。
- 通过删除将 print_blob 设置为 PrintSettings 的选项，简化了逻辑。
- 改进了 domains（）策略，以及使用它的 url（）和 emails（）策略。
- from_type（）策略现在知道查找抽象类型的子类，这些子类不能直接实例化。
- 改进了 from_lark（）策略，加强了参数验证，并添加了 explicit 参数，以允许与使用@declare 而不是字符串或正则表达式的终端一起使用。
- 在 byte_string_dtypes（）和 unicode_string_types（）中弃用 0 的 min_len 或 max_len。现在的下限是 1。
- 如果在非交互式上下文中使用策略的.example（）方法，将发出警告。
- 添加了 hypothesion.target（）函数，该函数实现了有针对性的基于属性的测试。
- 添加了 basic_indices（）策略，为指定形状的数组生成基本索引。
- 升级了 fixed_dictionaries（）策略以支持可选密钥。
- 添加了 mutually_broadcastable_shapes（）策略，该策略生成多个阵列形状，这些形状与可选的用户指定的基本形状相互广播兼容。
- 为 mutually_broadcastable_shapes（）添加了一个签名参数。
- 在 from_type()支持 typing.Final 和 typing.TypedDict 。
- 更改了 floats（）在排除有符号零时的行为。
- 在运行显式示例和正常测试执行之间通用了一些代码。这对用户可见的主要影响是，现在在运行显式示例时强制执行截止日期。
- 通过使用一种名为 Swarm 测试的技术来选择在任何给定的测试用例中运行

哪些规则，显著改进了基于规则的状态测试中的数据分布。

- 如果设置为 0，将更改 stateful_step_count 设置以引发错误。这是一个向后兼容的更改，因为值 0 永远不会起作用，尝试运行它会导致内部断言错误。
- 增加了对基于目标属性的测试的数据库支持，因此基于目标的最佳示例将在运行之间保存和重用。
- 改进了在 from_type（ ）上对 SupportsOp 协议的支持。

5.7.282. python-importlib-metadata：

- 不再支持 python3.4
- Distribution._local() 隐形要求安装 pep517
- 优化代码，更好地与 stdlib 实现兼容
- 优化代码，增加系统容错性
- 优化代码，提升 FastPath 与 distribution()的性能
- 优化代码，PathNotFoundError 现在有一个自定义的__str__，其中提到缺少“包元数据”，以帮助用户在安装了包但没有元数据时找到原因
- 优化代码，在 EntryPoint 添加了模块和属性
- 优化文档
- 优化测试用例，提高 contextlib 和 pathlib 的可靠性和一致性
- 新增依赖接口：provides python3-importlib-metadata

5.7.283. python-incremental：

- 升级 incremental 到 21.3.0

5.7.284. python-jmespath：

- 移除 python2 子包
- 升级 jmespath 到 0.9.3

5.7.285. python-keyczar：

- 新增 python3-keyczar 模块

5.7.286. python-kitchen：

- 移除 python2-kitchen 子包

5.7.287. python-logutils：

- 新增 Provides：python-logutils

5.7.288. python-markdown：

- 增加新的 provides 依赖关系：python-markdown

5.7.289. python-marshmallow：

- 向字段添加格式参数。时间和时间格式类 Meta 选项。
- 强制转换为 Mapping.serialize 和 Mapping 中的映射类型。
- 通过关键字参数传递字段元数据已弃用，并将在 marshmallow 4 中删除。使用显式 metadata=...参数。

- 添加字段。IPInterface，字段。IPv4Interface 和 IPv6Interface。
- 使用字段时，对缺少的方法提出 AttributeError。
- 删除 Field 中不必要的 hasattr 和 getattr 检查。
- 向 marshmallow.decorators 添加类型注释
- 改进 marshmallow.validate 中的类型。
- 使 marshmallow.validate.Validator 成为抽象基类。
- 删除不必要的列表强制转换。
- 将缺失/默认字段参数替换为 load_default/dump_default。
- 弃用：缺失/默认字段参数的使用已弃用，并将在 marshmallow 4 中删除。

  应改用 load_default/dump_default。
- 改进了将元数据作为关键字参数传递时的警告。
- 不再支持 Python 2、放弃对 Python 3.5 的支持。
- 允许将字典传递给字段。
- 将 py310 添加到 black target-version 中。
- 放弃对 Python 3.6 的支持。
- 使用注释的延迟评估。
- 支持在 TimeDelta 字段中序列化为 float。
- 将 messages_dict 属性添加到 ValidationError 中，以便于类型检查。
- 向字段添加时间戳和 timestamp_ms 格式。
- 将绝对参数添加到 URL 验证器和 Url 字段。
- 使用抽象基类定义 FieldABC 和 SchemaABC。
- 使用 OrderedSet 作为默认 set_class。架构现在是默认排序的。

- 在 utils.from_timestamp 中处理 OSError 和 OverflowError。
- 正式支持 Python 3.11、放弃对 Python 3.7 的支持。

5.7.290. python-meh：

- 为了防止更高版本出现问题，在计算哈希时使用异常的类型和值来区分不同的错误现象
- 新增拆分出的 python3-meh-gui 子包

5.7.291. python-more-itertools：

- 增加 ilen 的实现注释；

5.7.292. python-netaddr：

- 修改 netaddr 敏感词问题

5.7.293. python-paramiko：

- 更新配置文件读取后返回的格式；
- 修改密钥注释长度导致的 SSHException 异常；
- ssh_config 解析期间执行 IdentityFile 内容去重
- 新增元数据信息：PKG-INFO 文件添加元数据

5.7.294. python-paste-deploy：

- * 添加了“setuptools”作为显式依赖项。这一直是必需的，但现在越来越多

的环境能够在不安装的情况下运行，我们现在需要确保它可用。

- * 删除了 pytest-runner，使用 tox 运行测试。
- python-webtest 在构建中发现缺少依赖，需要为 python-webtest 构建添加 python-PasteDeploy 的 python2 子包，同时删除 python-PasteDeploy 的 help 子包。

5.7.295. python-path：

- 新增 provides：python-path

5.7.296. python-pexpect：

- 禁用超时和 EOF 异常的链接；
- 允许通过 str_last_chars 配置回溯包含的代码片段长度，而不是总是 100；
- 如果提供了 ssh 配置，pxssh.login()方法现在不再需要用户名，如果两者都不提供，则会引发错误；
- pxssh.login()方法支持通过 cmd 参数提供 ssh 命令；
- pxssh 现在支持 use_poll 参数，该参数传递给 pexpect.spawn() ；
- replwrap.run_command()现在通过 async_参数支持异步；
- 如果能够达到缓冲区限制，expect.spawn()现在将读取额外的字节；

5.7.297. python-pillow：

- 升级到 9.0.1 版本

5.7.298. python-pyasn1：

- 添加了以前缺少的 SET OF ANY 构造编码/解码支持；
- 添加.reset()方法以将值对象转换为架构对象等。
- 新增结构体，添加更多调试日志记录：
- 删除过时的 python-pyasn1-modules

5.7.299. python-pytest-expect：

- 根据宏的存在来提供 python3-pytest-expect

5.7.300. python-pytest-xdist：

- 新增特性，pytest 支持 pdb 调试；
- 使用 pytest -ff -n=auto ... 进行单元测试时会提示 UsageError；
- 增加 pytest_xdist_getremotemodule，用于覆盖远程节点使用的模块；
- 在调用远程节点的模块时，可通过 pytest_xdist_getremotemodule 来 wrap 该模块的调用；
- 打印警告信息时，使用 DumpError 来显示更多的详细描述信息；
- 适配 pytest4.1 中关于 ExceptionInfo 、pytest_logwarning 两个 API 的变化；
- 功能增强，在 quite 模式下不再显示 setup 结果的消息；
- 新增—maxprocesses 选项，用于在--numprocesses=auto 时限制最大的工作节点

5.7.301. python-SecretStorage：

- 增加判断，在 python2 环境用 int_from_bytes，在 python3 环境用 int.from_bytes

5.7.302. python-sortedcontainers：

- 新增实现 SortedDict 方法__or__，__ror__，__ior__
- 在使用大型可迭代项进行更新时，使排序顺序稳定
- 新增 python2-sortedcontainers 安装包
- 卸载软件包时删除缓存目录

5.7.303. python-sphinx：

- 适配 jQuery 版本升级后的接口变动

5.7.304. python-sure：

- 新增编译依赖：python2-mock python2-nose python-setuptools python2-six python2-setuptools

5.7.305. python-tornado：

- 新增二进制包 python-tornado

5.7.306. python-urllib3：

- 将 server_hostname 添加到 SSL_KEYWORDS。

5.7.307. python-virtualenv：

- 修改安装依赖关系、新增：python3-appdirs python3-distlib python3-filelock python3-importlib_metadata

5.7.308. qpid-proton：

- 新增 python2 支持，新增子包 python2-qpid-proton

5.7.309. qt5-qtbase：

- 增加 loongarch64 架构支持。

5.7.310. qt5-qtmultimedia：

- 删除二进制文件的 rpath 属性

5.7.311. qt：

- 增加 loongarch64 架构支持。
- 增加 zh_HK 繁体翻译。

5.7.312. quota：

- 优化 prep 处理逻辑，将 autoreconf 文件内容的生成移到 build 中。
- 新增支持申威架构。

- quotacheck，quotaon：支持 ext4 使用配额功能。
- Quota：增加 --filesystem 选项 。
- 处理 XFS 支持超过 2038 年的宽限期到期。
- 配额工具：为单个 xfs 宽限时间设置 FS_DQ_TIMER_MASK。
- 配额工具：将配额类型传递给 Q_XFS_GETQSTAT 的 QCMD
- warnquota：初始化 configparams 结构的所有成员
- warnquota：免费 LDAP 错误消息
- 使 quota_nld PID 文件的目录可配置。
- warnquota：还打印 LDAP 错误的其他错误信息。
- warnquota：正确检测 LDAP 错误
- warnquota：不要忽略配置文件中的错误
- quotacheck：跳过早期检查具有隐藏配额文件的文件系统
- quotaops：修改错误字符串的含义
- rpc:当无法连接到 rpc.rquotad 时澄清错误消息
- setquota：报告获取配额信息失败
- quotaops：结构发生故障时不要泄漏
- quotaops：不从 getprivas 返回部分列表。
- 使有关 NFS 故障的消息与本地文件系统保持一致
- edquota：删除忘记的许可证标头
- config.ac:增加--disable-pie 选项
- 避免篡改用户 CFLAGS

5.7.313. rarian：

- 移除可执行文件的 rpath/runpath 属性值

5.7.314. rasdaemon：

- 延长文件访问等待。
- 修改在 rasdaemon 中记录海思常见错误数据。
- 适应内核链路环缓冲区的变化。
- ras-events：当 KBUF 数据被破坏时，read_ras_event 退出循环。

5.7.315. rdma-core：

- 新增 loongarch64 架构支持；

5.7.316. re2：

- 添加一些针对不常用分支的测试用例。

5.7.317. realmd：

- 0.16.3 -> 0.17.0：

  支持 automake 0.16 版本

  realm 命令的 discover, join 和 leave 新增--use-ldaps 选项，使 realmd 服务能使用 ldaps

  service:在使用 adcli 时添加 ldaps 支持

service:允许使用 ldaps 进行 rootDSE 查找

- 0.17.0 -> 0.17.1：

  tools:为 AD 添加--do-not-touch-config 选项

  ldap:添加 socket 超时

  将计算机名称添加到 realm man 手册页

  更新 autoconf-2.71 的一些宏

  添加--with-vendor-error-message 配置选项

5.7.318. redis：

- 禁止副本运行 replicaof 命令。
- 重写 BRPOPLPUSH 为 RPOPLPUSH 以进行传播。
- 不将不支持的协议视为致命错误。

5.7.319. redland：

- 用 mariadb-connector-c-devel 替换 mysql-devel

5.7.320. rootsh：

- rootsh --help 和 man rootsh 中显示的帮助信息不一致，因此将 rootsh 的参数“-?”修改为“-h”

5.7.321. rpcbind：

- 代码编译默认启用远程调用功能，并增加参数-r，通过参数可配置启用或者禁用
- 默认关闭 rpcbind.service 服务

5.7.322. rpmrebuild：

- 当输入-k 参数时重置 defattr
- 当输入--change-files 时修改目录 uid 和 gid

5.7.323. rpm：

- 添加 loongarch 架构支持
- 添加麒麟安全补丁

5.7.324. samba：

- 使用 chrpath 命令移除 so 库文件和二进制文件的运行时搜索路径（run-time search path），使用默认的运行时库搜索路径来查找依赖的共享库。

5.7.325. sane-backends：

- 新增 lib/statuskysec.c、include/statuskysec.h 文件，用来获取判断系统白名单以及子项设备管控状态。

5.7.326. sanlock：

- sanlk-reset 命令新增-t 选项

- 添加 python3-sanlock 子包

5.7.327. scap-security-guide：

- 增加规则文件，以支持麒麟系统安全检测

5.7.328. scap-workbench：

- 删除了不建议使用的 Qt4 调用

5.7.329. sed：

- 使用 char *替代废弃的 security_context_t，避免产生新的告警；
- 替换 configure.ac 中过时的构建选项（AM_CONFIG_HEADER 替换为 AC_CONFIG_headersAC_PROG_CC,AC_PROG_CC_STDCAC_TRY_RUN 替换为 AC_RUN_IFELSE），避免 autoconf 告警；
- 关闭临时文件失败时，do_ck_fclose 会尝试同时执行 fclose 并对同一个文件指针 unlink,这一双重关闭行为会导致 panic，这一潜在问题会被-Wanalyzer-double-fclose 捕获，修改其行为当 fclose 失败时调用 mark_as_fclose_failed；

5.7.330. sendmail：

- sendmail.service 服务启动之后 pid 报错
- sendmail.pem 用于服务器，普通用户无需权限；

- sendmail 安装后 sendmail.pem 证书有效期小于 1 年；

5.7.331. setroubleshoot：

- 完善繁体中文支持

5.7.332. sg3_utils：

- 加速多路径设备扫描速度
- 加快 rescan 扫描流程

5.7.333. shared-mime-info：

- 优化繁体中文支持

5.7.334. shim：

- 在可信计算 3.0 双体系框架下，麒麟系统侧增加支持与防护部件的通信
- 增强安全性：OS 支持商密安全启动，shim 组件支持 SM3 摘要计算和 SM2 签名校验
- 更新使用说明、配置指南和故障排除指南
- 新增支持支持 loongarch64 架构
- 新增支持 RSA 与国密证书的安全启动

5.7.335. sleuthkit：

- 移除已衰退的依赖包 mac-robber

5.7.336. squashfs-tools：

- mksquashfs 现在支持“Actions”。这些是以“find”并允许压缩、碎片打包、文件排除和要更改的文件属性。
- 新的 sqfstar 命令将从 tar 档案创建 squashfs 格式的 image 文件。
- 对 mksquashfs 中源路径名的 Tar 风格处理。
- 对 mksquashfs 中源路径名的 Cpio 风格处理。
- 限制 CPU 和 I/O 数量的新选项。
- 支持时间戳的新 Pseudo 文件定义。
- 创建文件引用的新 Pseudo 文件定义。
- 创建 Sockets/Fifos 的新 Pseudo 文件定义。
- mksquashfs 现在不允许指定任何源目录。
- 允许常规文件的新 Pseudo 文件“R”定义以与存储在伪文件内的数据一起创建。
- Sqfscat 命令，用于将文件输出到 stdout。
- 现在提取文件中遵循符号链接（使用-遵循符号链接或-缺少符号链接）。
- unsquashfs 现在支持“exclude”文件。
- 增加了最大深度遍历选项。
- unsquashfs 现在可以输出一个“Pseudo file”，表示输入 Squashfs 文件系统。
- 现在显示并更新进度条，同时正在扫描输入。
- mksquashfs 新增 -one-file-system 选项。
- mksquashfs 新增 -no-hardlinks 选项。
- mksquashfs 和 unsquashfs 新增多处 help 帮助信息。

- mksquashfs 新增 -root-uid 选项。
- mksquashfs 新增 -root-gid 选项。
- mksquashfs 新增 -root-time 选项。
- unsquashfs 新增 -no-exit-code 选项，这使它不输出错误退出代码。
- unsquashfs 中的 exit code 已更改以区分非致命错误（exit2）和致命错误（exit 1）。
- mksushfs 在追加时，现在将恢复文件写入 home 目录，而不是当前目录。
- 新增 -recovery-path＜name＞选项。
- unsquashfs“-stat”输出中添加的 Xattr id 计数。
- 防止 mksquashfs 读取目标文件。

5.7.337. star：

- 将 pax.1.gz 文件从 star 包挪到 star-help 包,

5.7.338. sudo：

- 在 sudoers_parse_ldif 函数中，可能读到未定义的内存
- 在 sudo_passwd_cleanup 函数中，auth-data 在 free 之后没有赋 NULL
- 增加 sw64 架构支持

5.7.339. supermin：

- 添加-pie -Wl,-z,now 安全编译参数

5.7.340. syslinux：

- syslinux-extlinux.rpm 二进制软件包中增加打包文件 extlinux*。

5.7.341. system-config-printer：

- 港澳繁体翻译修改

5.7.342. systemd：

- 移除可执行文件的 rpath/runpath 属性值、提升安全；
- 添加一些内存 overflow 溢出检查
- 使每个标签以 nul 终止，防范 dns_label_unescapetriggers 缓冲区溢出
- 添加出错后正常 return 返回动作
- udev 日志增加 udev rules 文件的 mode 属性打印
- udevadm 中启用 usec_add()
- 优化 install_context_apply()的错误码
- udevadm trigger 模块优化返回码的处理
- 增加 pstore 中 dmesg 信息存储状态检查
- 优化 udev 规则属性文件中的换行符处理
- 优化 udev 退出时对 workers 的等待处理
- 优化 systemd 对 daemon 程序的 trigger 逻辑条件
- udevadm trigger 中增加忽略 EROFS

- 优化 sd-event 模块中其他线程对默认事件循环不执行
- time-util 模块增加支持用户空间的 time_t 是 64 位但是内核不是的系统
- time-util 模块对 EOVERFLOW 错误处理中增加 32 位长的处理
- 优化 udev 规则文件的匹配逻辑中的文件权限设定
- 优化 udev 网络对 bit rate 的存储、全部由改为 uint_64_t
- 为 systemd-networkd.service 增加 AF_ALG、满足 Khash 需求
- udevadm info 增加更多的错误信息展示
- udevd 避免杀死运行中的 worker 进程
- 优化 Exec* 指令中的“+”前缀处理逻辑、忽略 PrivateTmp 等文件系统方面的选项
- journalctl 命令新增功能参数--facility=kern；
- journal 执行失败增加打印日志；
- 切换 su 到普通用户，执行 busctl 命令时增加 Interactive authentication 回显；

5.7.343. tboot：

- 释放 S3 流中用于 CRB 接口的位置。在执行 GETSEC [SENTER]之前，必须释放位置 0，在跳到 Linux 内核之前，必须释放位置 2。
- 在生成 tboot.gz 之前剥离可执行文件
- 添加对 EFI 内存映射解析/修改的支持。
- lcptools-v2：添加 pconf2 策略元素支持。
- tb_polgen：添加 SHA384 和 SHA512 支持。

- 禁用 GCC9 打包成员地址警告：GCC9 引入了导致构建失败的新警告，允许对内存进行未对齐的访问（导致性能下降），可以禁用警告而不会导致 CPU 故障。
- 使用 SHA256 作为默认哈希算法：如果用户未提供任何配置，则 TBOOT 将选择 SHA256，而不是此提交之前的 SHA1。
- tb_polgen：添加对 SHA256 的支持
- 在执行 GETSEC [SENTER]之前配置 IOMMU。
- 增加检查 size 时允许 SINIT ACM 填充。CBnT 规范定义了从 64kB 到 256kB 的 SINIT 填充，为了与旧平台兼容，TBOOT 也接受不带填充的 SINIT。
- 添加对 64 位帧缓冲区地址的支持。启用> 4GB MMIO 后，EFI 可以返回超过 32 位边界的帧缓冲区地址，TBOOT 必须正确地将 64 位地址传递给 Linux 内核。
- 将 SM3 算法添加为 tboot 中的嵌入式支持。
- 添加 safestringlib 代码以替换被禁止的 mem/str fns
- lcptools：删除 2008 年之前支持平台的工具。
- tboot：更新 tring/memory fn 名称以区别于 c lib
- 添加选项 save_vtd = true 以选择加入 vtd 表还原:acpi 表似乎已被内核更改。
- 恢复变更集 522：8e881a07c059 中的错误更改类型转换。

5.7.344. tcpdump：

- 新增支持 RDMA 网络报文捕获
- 新增多种协议的支持
- 新增—micro 与 –nano 参数，用于解析抓包文件时更改显示的时间戳格式
- 新增—print 参数，可在指定 output 文件的同时，将抓包内容显示到 stdout 中
- 新增支持 sw64 架构
- 新增信号捕捉(REQ_INFO，FLUSH_PCAP)，避免在试用管道写入二进制抓包文件时由于 write()系统调用没有重置，导致损坏 pcap 输出
- 新增 Offloaded Traffic Sniffer 功能（针对 MLX ConnectX®-4 以上的版本），可捕获 bypass kernel 的数据包

5.7.345. tigervnc：

- 添加了港澳繁体中文翻译支持

5.7.346. tpm-tools：

- 删除二进制中的 rpath 属性设置

5.7.347. traceroute：

- 将 IPv4(::ffff:A.B.C.D) 映射的 IPv6 地址解释为真正的 IPv4 地址
- 实现更健壮的轮询（poll）循环处理

5.7.348. tree：

- 为 --du 和 --prune 这两个参数添加帮助信息

5.7.349. ttmkfdir：

- 在编译阶段增加 -fPIE 选项，以及在链接目标文件时增加-pie 选项,为了生成位置无关的可执行文件

5.7.350. tuna：

- 对安装依赖进行修改，将安装依赖 python2-ethtool、python2-schedutils >=0.2 更新为 python3-ethtool、python3-schedutils >=0.6。由依赖 python2 对应的软件包变更为依赖 python3 对应的软件包，增加 tuna 软件包的稳定性。

5.7.351. tzdata：

- 升级 tzdata 到 2022a-15 版本，同步最新更新全球各地时区及夏令时规则

添加编译命令，额外生成 main.zi 文件。

5.7.352. ukui-screensaver：

- 禁止在其他桌面环境启动；

5.7.353. unbound：

- 删除没用的旧库：libunbound.so.2；

5.7.354. units：

- 增加软件包安装依赖：python3-requests
- 更新货币时支持不同的数据源

5.7.355. usb_modeswitch-data：

- 新增对多个设备的支持

5.7.356. vala：

- provides 增加 vala-tools
- 删除二进制文件的 rpath 属性

5.7.357. vdo：

- 修改了工具本身以正确转换 UDS 索引，从而重复数据消除信息不会因转换而丢失;
- 向 vdopreparelvm 添加了一个检查，以确定它是否已经转换;

5.7.358. vim：

- Kylin 的产品化修改内容，包括敏感词修改、zh_HK 繁体字支持等功能

5.7.359. virglrenderer：

- 修改部分函数公共接口为私有接口

- 公共接口添加部分功能
- 增加对视频编解码器的支持

5.7.360. vorbis-tools：

- 新增解码 ogg123 中的 METADATA_BLOCK_PICTURE 标签支持
- 增加了对从 blob 中解析 flac 图片的支持
- 去除 elf 文件中的 rpath 属性，提升安全

5.7.361. watchdog：

- 添加 ipmi 服务顺序依赖项;
- 删除变量的双重清除；
- 添加单独的 swap 使用测试：允许在 swap 空间使用过多时重新启动；将 swap 使用测试从最小可用内存测试中分离出来；
- 更新内存测试文档；
- 从 free+buffers+cache 中计算可用内存；
- 将字符串解析移动到函数调用；
- 对 kB 值使用长整型；
- 允许足够的空间读取所有/proc/meminfo；
- 在配置文件中增加 SIGTERM 延迟；
- 更新示例 watchdog.conf 文件：重新排序文件，将硬件设置放在首位；包括可设置参数的更多示例；文件中有更多的文档来帮助使用；
- 增加配置选项，忽略 watchdog 错误：允许看门狗简单地忽略写入看门狗设备时遇到的错误；

- 将最小刷新时间设置为 0.2s（原设置为 0.5s）；
- 移除主循环之前的延迟；

5.7.362. wxGTK3：

- 增加 loongarch64 架构支持；
- wxBase3-devel 安全编译选项 PIE 不满足；

5.7.363. xcb-util-keysyms：

- 使用 xz 替换 bzip2

5.7.364. xfsdump：

- 把软件包文档中的“slave”单词移除，改为“worker”
- 移除 DMAPI 的支持

5.7.365. xinetd：

- 添加对 sw64 架构的支持
- xinetd.service 配置文件，添加 Restart=on-failure 项

5.7.366. xkeyboard-config：

- 增加繁体翻译

5.7.367. xnio：

- 单元测试用例优化

5.7.368. xorg-x11-drv-vesa：

- 增加对 loongarch64 架构的支持

5.7.369. xorg-x11-xinit：

- 删除无用文件 xinit-compat.desktop

5.7.370. xz：

- 用户交互优化，给 xzgrep、xzegrep、xzfgrep 命令配置颜色

5.7.371. yajl：

- 优化变量的内存分配逻辑，增加对分配失败的处理

5.7.372. yhkylin-backup-tools：

- 繁体界面和繁体翻译

6. 附录 2 重要的安全漏洞修复

漏洞	漏洞描述	等级
CVE-2023-30577	Amanda 是 University of Maryland at College Park 组织的一种自动网络磁盘存档器。允许 IT 管理员设置单个主备份服务器，以通过网络将多个主机备份到磁带驱动器/转换器或磁盘或光学介质。\ramanda 3.5.4 之前版本存在安全漏洞，该漏洞源于 AMANDA (Advanced Maryland Automatic Network Disk Archiver) 错误处理了 runtar.c 的参数检查。	重要
CVE-2023-24998	Apache Commons FileUpload 是美国阿帕奇（Apache）基金会的一个可将文件上传到 Servlet 和 Web 应用程序的软件包。	重要

	Apache Commons FileUpload 1.5 之前版本存在安全漏洞，该漏洞源于没有限制请求的数量，从而导致系统拒绝服务。	
CVE-2022-45047	Apache MINA 是美国阿帕奇（Apache）基金会的一款网络应用程序框架。该产品主要用于开发高性能和高可伸缩性的网络应用程序。\rApache MINA 2.9.1 及之前版本存在代码问题漏洞，该漏洞源于 使用 Java 反序列化加载序列化 java.security.PrivateKey，攻击者利用该漏洞可以选择加载一个主机密钥 SSH 服务器。	严重
CVE-2022-24963	Apache Portable Runtime（APR,Apache 可移植运行库）是美国阿帕奇（Apache）基金会的一个为上层应用程序提供可跨越多个操作系统平台使用的底层支持接口库。\rApache Portable Runtime(APR) 1.7.0 版本存在输入验证错误漏洞，该漏洞源于其 apr_encode 函数允许攻击者实现整数溢出或环绕错误导致向缓冲区边界之外写入数据。	严重
CVE-2022-47630	Linaro Trusted Firmware-A 是 Linaro 开源的一种可信固件。\rLinaro Trusted Firmware-A 2.8 及之前版本存在安全漏洞，该漏洞源于在解析引导证书的 X.509 解析器中存在越界读取，攻击者利用该漏洞可能会触发读取或获取有关微架构状态的敏感信息。	重要
CVE-2022-41704	Apache XML Graphics Batik 是美国阿帕奇（Apache）基金会的一套基于 Java 的主要用于处理 SVG 格式图像的应用程序。\rApache XML Graphics Batik 1.16 之前版本存在安全漏洞，该漏洞源于 Batik 存在问题，允许攻击者从 SVG 运行不受信任的 Java 代码。	重要
CVE-2022-42890	Apache XML Graphics Batik 是美国阿帕奇（Apache）基金会的一套基于 Java 的主要用于处理 SVG 格式图像的应用程序。\rApache XML Graphics 1.16 之前版本存在安全漏洞，该漏洞源于 Batik 存在问题，允许攻击者通过 JavaScript 从不受信任的 SVG 运行 Java 代码。	重要
CVE-2023-3341	miniCal 是 miniCal 开源的一款开源的 PMS。\rminiCal 1.0.0 及之前版本存在安全漏洞，该漏洞源于包含 CSV 注入漏洞，允许攻击者远程执行代码。	重要
CVE-2023-2828	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。 ISC BIND 9 存在安全漏洞，该漏洞源于缓存配置限制不当，攻击者利用该漏洞可以导致拒绝服务条件。	重要
CVE-2022-2906	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。ISC BIND 9.18.7 之前的 9.18.x 版本、9.19.5 之前的 9.19.x 版本存在安全漏洞，该漏洞源于 OpenSSL 1.x 和 OpenSSL 3.0 之间的更改暴露了命名中的一个缺陷，当在 Diffie-Hellman 模式下与 OpenSSL 3.0.0 及更高版本一起使用 TKEY 记录时，该缺陷会导致密钥处理中出现少量内存泄漏。攻击者可以利用此漏洞逐渐侵蚀可用内存，以至于命名的内存因缺乏资源而崩溃，重新启动后，攻击者将不得不重新开始，但仍有可能拒绝服务。	重要
CVE-2022-2881	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。ISC BIND 9.18.7 之前的 9.18.x 版本、9.19.5 之前的 9.19.x 版本存在安全漏洞，该漏洞源于重用 HTTP 连接从 stats 通道请求统计信息时，连续响应的内容长度可能会增长到超过分配缓冲区的末尾，可能会导致读取超出缓冲区的末尾并读取它不应该读取的内存，或者使进程崩溃。	重要
CVE-2022-2795	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。ISC BIND 9.16.33 之前版本、9.18.7 之前的 9.18.x 版本、9.19.5 之前的 9.19.x 版本存在安全漏洞，该漏洞源于解析器代码中的缺陷可能会导致命名在处理大型委托上花费过多的时间,攻击者通过利用此漏洞向目标解析器充斥查询，可以显着削弱解析器的性能，从而有效地拒绝合法客户端访问 DNS 解析服务。	重要
CVE-2022-38178	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。BIND 存在安全漏洞，该漏洞源于使用格式错误的 EdDSA 签名，欺骗目标解析程序，导致内存因资源不足而崩溃。以下产品及版本受到影响:9.9.12 版本至 9.9.13 版本、9.10.7 版本至 9.10.8 版本、9.11.3 版本至 9.16.32 版本、9.18.0 版本至 9.18.6 版本、9.19.0 版本至 9.19.4 版本。	重要
CVE-2022-38177	ISC BIND 是美国 ISC 公司的一套实现了 DNS 协议的开源软件。ISC BIND 9.8.4 版本至 9.16.32 版本存在安全漏洞，该漏洞源于使用格式错误的 ECDSA 签名，欺骗目标解析程序，导致内存因资源不足而	重要

	崩溃。	
CVE-2022-47008	GNU Binutils（GNU Binary Utilities 或 binutils）是美国 GNU 社区的开发的一组编程语言工具程序。该程序主要用于处理多种格式的目标文件，并提供有连接器、汇编器和其他用于目标文件和档案的工具。GNU Binutils 存在安全漏洞，该漏洞源于 bucomm.c 文件中的 make_tempdir 和 make_tempname 函数存在内存泄漏问题。	重要
CVE-2022-47011	GNU Binutils（GNU Binary Utilities 或 binutils）是美国 GNU 社区的开发的一组编程语言工具程序。该程序主要用于处理多种格式的目标文件，并提供有连接器、汇编器和其他用于目标文件和档案的工具。GNU Binutils 存在安全漏洞，该漏洞源于 stabs.c 文件中的 parse_stab_struct_fields 函数存在内存泄漏问题。	重要
CVE-2022-47696	GNU Binutils（GNU Binary Utilities 或 binutils）是美国 GNU 社区的开发的一组编程语言工具程序。该程序主要用于处理多种格式的目标文件，并提供有连接器、汇编器和其他用于目标文件和档案的工具。\rGNU Binutils 存在安全漏洞，该漏洞源于 objdump 工具中的 compare_symbols 函数可以导致拒绝服务。	重要
CVE-2021-46174	GNU Binutils（GNU Binary Utilities 或 binutils）是美国 GNU 社区的开发的一组编程语言工具程序。该程序主要用于处理多种格式的目标文件，并提供有连接器、汇编器和其他用于目标文件和档案的工具。GNU Binutils 存在安全漏洞，该漏洞源于 bfd_getl32 函数存在堆溢出漏洞。	重要
CVE-2022-39176	BlueZ 是一款使用 C 语言编写的蓝牙协议堆栈，它主要用于提供对核心蓝牙层和协议的支持。BlueZ 5.59 之前的版本存在安全漏洞，该漏洞源于 profiles/audio/avrcp.c 组件不能验证 params_len 导致近源攻击者可以获取敏感信息。	重要
CVE-2022-39177	BlueZ 是一款使用 C 语言编写的蓝牙协议堆栈，它主要用于提供对核心蓝牙层和协议的支持。BlueZ 5.59 之前的版本存在安全漏洞，该漏洞源于 profiles/audio/avdtp.c 组件可以处理畸形和无效的功能导致近源攻击者可以获取敏感信息。	重要
CVE-2023-27349	该漏洞源于 AVRCP 协议处理中存在边界错误，远程攻击者可以向受影响的系统发送特制的蓝牙数据包，触发内存损坏并在系统上执行任意代码。	重要
CVE-2023-32067	当目标解析器发送查询，攻击者伪造一个长度为 0 的畸形 UDP 报文返回给目标解析器。目标解析器错误地将 0 长度理解为连接的正常关闭，解析失败，实现 DoS 攻击，拒绝服务。	重要
CVE-2020-27781	OpenStack 是美国国家航空航天局（National Aeronautics and Space Administration）和美国 Rackspace 公司合作研发的一个云平台管理项目。OpenStack Manila 存在安全漏洞，该漏洞源于 DescriptionUser 凭据可能会被 OpenStack Manila 的本地 CephFS 消费者操纵和窃取，从而导致潜在的特权升级。	重要
CVE-2020-10753	Ceph 是一套 Linux PB 级分布式文件系统。该系统的主要目标是设计成基于 POSIX（可移植操作系统接口）的没有单点故障的分布式文件系统，使数据能容错和无缝的复制。Ceph 3.x 版本和 4.x 版本中的 RadosGW 存在注入漏洞。该漏洞源于用户输入构造命令、数据结构或记录的操作过程中，网络系统或产品缺乏对用户输入数据的正确验证，未过滤或未正确过滤掉其中的特殊元素，导致系统或产品产生解析或解释方式错误。	重要
CVE-2021-3524	该漏洞与通过 CORS ExposeHeader 标签注入 HTTP 标头有关。当提出 CORS 请求时，CORS 配置文件中 ExposeHeader 标记中的换行符会在响应中产生头注入。此外，之前针对 CVE-2020-10753 的漏洞修复没有考虑到使用 \r 作为头分隔符的情况，因此产生了一个新漏洞。	重要
CVE-2020-1760	Ceph 是一套 Linux PB 级分布式文件系统。该系统的主要目标是设计成基于 POSIX（可移植操作系统接口）的没有单点故障的分布式文件系统，使数据能容错和无缝的复制。 Ceph Object Gateway 中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。	重要
CVE-2022-27239	cifs-utils 是 Pavel Shilovsky 个人开发者的一个工具包。提供用于管理 CIFS 网络文件系统安装的实用程序。piastry cifs-utils 存在安全漏洞，该漏洞源于应用在解析 mount.cifs ip=命令行参数时存在基于堆	重要

	栈的缓冲区溢出。本地攻击者利用该漏洞可以获得 root 权限。	
CVE-2023-20032	ClamAV 1.0.0 及更早版本、0.105.1 及更早版本和 0.103.7 及更早版本的 HFS+分区文件解析器中的漏洞可能允许未经身份验证的远程攻击者执行任意代码。此漏洞是由于缺少缓冲区大小检查，可能导致堆缓冲区溢出写入。攻击者可以通过在受影响的设备上提交精心编制的 HFS+分区文件供 ClamAV 扫描来利用此漏洞。成功利用此漏洞可能使攻击者能够使用 ClamAV 扫描进程的权限执行任意代码，或者使进程崩溃，从而导致拒绝服务（DoS）情况。	严重
CVE-2023-20197	ClamAV（Clam AntiVirus）是 ClamAV 团队的一套免费且开源的杀毒软件。该软件用于检测木马、病毒、恶意软件和其他恶意威胁。\rClamAV Hierarchical File System Plus 存在安全漏洞，该漏洞源于在解压缩文件时错误地检查完成情况，可能允许未经身份验证的远程攻击者在受影响的设备上造成拒绝服务(DoS)。	重要
CVE-2022-4515	Ctags 是 Sourceforge 开源的一个用于从程序源代码树产生索引文件，从而便于文本编辑器来实现快速定位的实用工具。 Ctags 存在安全漏洞，该漏洞源于 sort.c 中的 externalSortTags()以不安全的方式调用 system(3)函数。	重要
CVE-2023-24805	CPUS 是一套开源打印系统。 CPUS cups-filters 存在操作系统命令注入漏洞，该漏洞源于可以使用操作数 cmdline 调用 system 命令。	重要
CVE-2022-26691	在 CUPS 打印系统中发现了一个授权漏洞。此安全漏洞发生在本地授权发生时。此漏洞允许攻击者在没有 32 字节密钥的情况下以 root/admin 身份向 CUPS 进行身份验证并执行任意代码执行。	重要
CVE-2023-38545	Curl 软件包中的 SOCKS5 代理握手中发现了一个基于堆的缓冲区溢出漏洞。如果 Curl 无法自行解析地址，它会将主机名传递给 SOCKS5 代理。然而，可以传递的主机名的最大长度为 255 字节。如果主机名过长，Curl 将切换到本地名称解析，并将解析后的地址仅传递给代理。在慢速 SOCKS5 握手期间，指示 Curl“让主机解析名称”的本地变量可能会获得错误的值，导致过长的主机名被复制到目标缓冲区，而不是解析后的地址，这并非预期行为。	重要
CVE-2022-24407	Cyrus Sasl 是 The Cyrus Team 团队的一种简单身份验证。使应用程序开发人员可以轻松地将身份验证机制以通用方式集成到应用程序中。Cyrus SASL 存在安全漏洞，该漏洞源于 Cyrus SASL SQL 插件错误地处理了 SQL 输入。远程攻击者可以利用此问题执行任意 SQL 命令。	重要
CVE-2018-25032	zlib 是美国 Mark Adler 个人开发者的一个通用的数据压缩库。zlib 1.2.11 版本存在缓冲区错误漏洞，该漏洞源于如果输入有很多远匹配，压缩时可能出现内存损坏。	重要
CVE-2022-37434	zlib 是美国 Mark Adler 个人开发者的一个通用的数据压缩库。zlib 1.2.12 版本存在安全漏洞，该漏洞源于在 inflate.c 中通过一个大的 gzip 标头额外字段在 inflate 中具有基于堆的缓冲区过度读取或缓冲区溢出。	重要
CVE-2021-25215	bind 中发现了一个缺陷。DNAME 记录的处理方式可能会触发将同一 RRset 添加到应答部分多次，从而导致断言检查失败。此漏洞的最大威胁是系统可用性。	重要
CVE-2022-2928	ISC DHCP 是美国 ISC 公司的一套开源的动态主机配置协议服务器软件。ISC DHCP 4.4.0 至 4.4.3 版本、4.1-ESV-R1 至 4.1-ESV-R16-P1 版本存在安全漏洞，该漏洞源于当从 add_option()调用函数 option_code_hash_lookup()时，它会增加选项的 refcount 字段，但是没有对 option_dereference()的相应调用来减少 refcount 字段，函数 add_option()仅用于服务器对租约查询数据包的响应，每个租约查询响应都会为多个选项调用此函数，因此最终，引用计数器可能会溢出并导致服务器中止。	重要
CVE-2022-2929	ISC DHCP 是美国 ISC 公司的一套开源的动态主机配置协议服务器软件。ISC DHCP 1.0 至 4.4.3 版本、4.1-ESV-R1 至 4.1-ESV-R16-P1 版本存在安全漏洞，该漏洞源于可以访问 DHCP 服务器的系统，发送经过精心设计的包含超过 63 个字节 fqdn 标签的 DHCP 数据包，最终可能导致服务器内存不足。	重要
CVE-2020-25681	在 dnsmasq 中发现一个缺陷。在使用 DNSSEC 数据进行验证之前，已按照对 RRSets 进行排序的方式发现了基于堆的缓冲区溢出。网络上的攻击者可以伪造 DNS 回复（例如被接受为有效的回复），可	重要

	以利用此缺陷导致堆内存段中任意数据的缓冲区溢出，从而可能在计算机上执行代码。此漏洞带来的最大威胁是对数据机密性和完整性以及系统可用性的威胁。	
CVE-2020-25682	Dnsmasq 是一款使用 C 语言编写的轻量级 DNS 转发和 DHCP、TFTP 服务器。 Dnsmasq 存在缓冲区错误漏洞，该漏洞源于在用 DNSSEC 数据验证 DNS 包之前，dnsmasq 从 DNS 包中提取名称的方式存在缓冲区溢出漏洞。	重要
CVE-2023-25173	containerd 是 containerd 开源的一个行业标准的容器运行时。 containerd 1.6.18 之前的 1.6.x 版本和 1.5.18 之前的 1.5.x 版本存在安全漏洞，该漏洞源于补充组在容器内没有被正确设置，攻击者利用该漏洞可能会获得对敏感信息的访问权限或获得在该容器中执行代码的能力。	重要
CVE-2023-28840	Moby 守护进程组件(dockerd)被开发为 Moby/Moby，通常被称为 Docker，其中 xt_u32 的关闭导致 docker 写 iptables 策略失败。	重要
CVE-2019-14584	在 tiancore EDK2 中解除空指针引用可能允许经过身份验证的用户通过本地访问潜在地启用权限提升。	重要
CVE-2021-38578	Tianocore Edk2 是 Tianocore 社区的一个遵循 UEFI 和 PI 规范的跨平台固件开发环境。Tianocore Edk2 存在安全漏洞，该漏洞源于在计算 BufferSize 时，SmmEntryPoint 中的现有 CommBuffer 检查不会捕获下溢。	重要
CVE-2022-4450	OpenSSL 是 OpenSSL 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 存在安全漏洞，该漏洞源于在 PEM_read_bio_ex 函数中存在双重释放漏洞，攻击者利用该漏洞可以提供恶意 PEM 文件进行解析以实现拒绝服务攻击。	重要
CVE-2023-0401	EDK II 是用于 UEFI 和 PI 规范的现代、功能丰富的跨平台固件开发环境。 在 PKCS7 签名或签名和信封数据上验证签名时，可以取消引用 NULL 指针。如果 OpenSSL 库已知用于签名的哈希算法，但哈希算法的实现不可用，则摘要初始化将失败。缺少对初始化函数返回值的检查，这将导致摘要 API 的无效使用，很可能导致崩溃。算法的不可用可能是由于使用启用 FIPS 的提供程序配置而导致的，或者更常见的原因是未加载旧版提供程序。PKCS7 数据由 SMIME 库调用和时间戳（TS）库调用处理。OpenSSL 中的 TLS 实现不会调用这些函数，但是如果第三方应用程序调用这些函数来验证不可信数据上的签名，则会受到影响。	重要
CVE-2023-0215	OpenSSL 是 OpenSSL 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 存在安全漏洞，该漏洞源于内存释放后重用。攻击者利用该漏洞导致程序崩溃，系统拒绝服务。	重要
CVE-2023-0286	OpenSSL 是 OpenSSL 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。 OpenSSL 存在安全漏洞，该漏洞源于内存释放后重用。攻击者利用该漏洞导致程序崩溃，系统拒绝服务。	重要
CVE-2022-45939	GNU Emacs 是美国 GNU 社区的一个文本编辑器家族。 GNU Emacs 28.2 版本及之前版本存在安全漏洞，该漏洞源于 lib-src/etags.c 在实现 ctags 程序时使用了系统 C 库函数。	重要
CVE-2022-48337	GNU Emacs 是美国 GNU 社区的一个文本编辑器家族。\rGNU Emacs 28.2 版本及之前版本存在操作系统命令注入漏洞。攻击者利用该漏洞通过源代码文件名称中的 shell 元字符执行命令。	严重
CVE-2022-48338	GNU Emacs 是美国 GNU 社区的一个文本编辑器家族。\rGNU Emacs 28.2 版本及之前版本存在安全漏洞，该漏洞源于在 ruby-mode.el 的 ruby-find-library-file 函数中发现包含本地命令注入漏洞。攻击者利用该漏洞可以执行任意命令。	重要

CVE-2023-28617	GNU Emacs 是美国 GNU 社区的一个文本编辑器家族。\rGNU Emacs Org Mode 9.6.1 版本及之前版本存在操作系统命令注入漏洞。攻击者利用该漏洞通过包含 shell 元字符的文件名或目录名执行任意命令。	重要
CVE-2022-25235	Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat（又名 libexpat）2.4.5 之前存在代码注入漏洞，该漏洞源于 xmltok_impl.c 缺少某些编码验证，例如检查 UTF-8 字符在特定上下文中是否有效。	重要
CVE-2022-25236	Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat（又名 libexpat）2.4.5 之前存在输入验证错误漏洞，该漏洞源于 xmlparse.c 允许攻击者将命名空间分隔符插入命名空间 URI。	重要
CVE-2022-25313	Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat 存在资源管理错误漏洞，该漏洞源于攻击者可以通过 DTD 元素中的较大嵌套深度触发 build_model 中的堆栈耗尽。	重要
CVE-2022-25314	Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat 存在安全漏洞，该漏洞源于在 2.4.5 之前的 Expat(又名 libexpat)中，copyString 中有一个整数溢出。	重要
CVE-2022-25315	Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat 存在输入验证错误漏洞，该漏洞源于 storeRawNames 中存在整数溢出。	重要
CVE-2022-40674	libexpat 是一款使用 C 语言编写的流式 XML 解析器。libexpat 2.4.9 之前的版本存在安全漏洞，该漏洞源于其 xmlparse.c 组件中的 doContent 函数存在释放后重用。	重要
CVE-2020-15969	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。WebRTC 是其中的一个支持浏览器进行实时语音对话或视频对话的组件。Chrome 存在安全漏洞。	重要
CVE-2020-15999	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 86.0.4240.111 之前版本中的 FreeType 存在缓冲区错误漏洞，攻击者可利用该漏洞可以通过 FreeType 的字体文件触发内存破坏，以触发拒绝服务，并可能运行代码。	重要
CVE-2022-22755	Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。Firefox 存在安全漏洞，该漏洞源于浏览器处理 XSL 文档的方式。攻击者可利用该漏洞欺骗受害者加载一个特别设计的 XSL 文档，该文档可以在同源策略的范围内继续执行 JavaScript，即使在浏览器选项卡关闭之后。	重要
CVE-2023-4863	在 Chromium 浏览器的 WebP 组件中发现堆缓冲区溢出缺陷。	重要
CVE-2023-5217	google chrome 浏览器中 117.0.5938.132 之前的版本所使用的组件 libvpx 存在堆溢出漏洞。该漏洞允许攻击者通过构建可触发漏洞的 HTML 页面实施攻击。	严重
CVE-2022-39320	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本可能会在太窄的类型上尝试整数相加，导致分配的缓冲区太小，无法保存写入的数据。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并将其发送回服务器。此问题在 2.9.0 版本中已解决，建议所有用户升级。无法升级的用户不应使用“/usb”重定向开关。	严重
CVE-2022-39317	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本在 ZGFX 解码器中缺少输入偏移索引的范围检查。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并尝试解码。此问题已在版本 2.9.0 中解决。对于这个问题，没有已知的变通办法。	严重
CVE-2022-39316	FreeRDP 是一个免费的远程桌面协议库和客户端。在受影响的版本中，在 FreeRDP 的 ZGFX 解码器组件中有一个超出限制的读取。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并尝试解码，这可能导致崩溃。这个问题在 2.9.0 版本中得到了解决。建议用户升级。	重要
CVE-2022-39318	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本在“urbdrc”通道中缺少输入验证。恶意服务器可以欺骗基于 FreeRDP 的客户端以除零崩溃。此问题已在版本 2.9.0 中解决。建议所有用户升级。无法升级的用户不应使用“/usb”重定向开关。	重要
CVE-2022-39319	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本可能会在太窄的类型上尝试整数相加，导致分配的缓冲区太小，无法保存写入的数据。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并将其发送回服务器。此问题在 2.9.0 版本中已解决，建议所有用户升级。无法升级	严重

	的用户不应使用“/usb”重定向开关。	
CVE-2022-39347	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本在“drive”通道中缺少输入长度验证。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并将其发送回服务器。此问题在 2.9.0 版本中已解决，建议所有用户升级。无法升级的用户不应使用驱动器重定向通道-命令行选项“/drive”，“+drives”或“+home-drive”。	重要
CVE-2022-41877	FreeRDP 是一个免费的远程桌面协议库和客户端。受影响的 FreeRDP 版本在“drive”通道中缺少输入长度验证。恶意服务器可以欺骗基于 FreeRDP 的客户端读取绑定数据并将其发送回服务器。此问题在 2.9.0 版本中已解决，建议所有用户升级。无法升级的用户不应使用驱动器重定向通道-命令行选项“/drive”，“+drives”或“+home-drive”。	严重
CVE-2022-39282	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。FreeRDP 2.8.1 之前版本存在安全漏洞，该漏洞源于在 unix 系统上基于 FreeRDP 的客户端使用/parallel 命令行开关可能会读取未初始化的数据并将其发送到客户端当前连接的服务器。	重要
CVE-2022-27404	FreeType 是一款使用 C 语言编写的开源字体渲染库。 FreeType 存在安全漏洞，该漏洞通过函数 sfnt_init_face 被发现包含堆缓冲区溢出。	严重
CVE-2022-27405	FreeType 是一款使用 C 语言编写的开源字体渲染库。FreeType 存在安全漏洞，该漏洞源于提交 53dfdcd8198d2b3201a23c4bad9190519ba918db 通过 FNT_Size_Request 函数发现包含分段违规。	重要
CVE-2022-27406	FreeType 是一款使用 C 语言编写的开源字体渲染库。FreeType 存在安全漏洞，该漏洞源于分段违规。	重要
CVE-2021-20240	gdk-pixbuf 是一款图像加载库。GDK-PixBuf 存在数字错误漏洞，攻击者可利用该漏洞可以触发一个整数溢出，导致拒绝服务，并可能运行代码	重要
CVE-2023-43115	ghostscript 到 10.01.2 中，GhostDL 中的 gdevijs.c 可以通过特制的 PostScript 文档导致远程代码执行，因为它们可以在激活 SAFER 后切换到 IJS 设备或更改 IjsServer 参数。注：可以在 gs 命令行上指定 IJS 服务器，这是一个记录在案的风险（IJS 设备本身必须执行命令才能启动 IJS 服务器）。	重要
CVE-2023-36664	Artifex Software Ghostscript 是美国 Artifex Software 公司的一款开源的 PostScript（一种用于电子产业和桌面出版领域的页面描述语言和编程语言）解析器。该产品可显示 Postscript 文件以及在非 Postscript 打印机上打印 Postscript 文件。\rArtifex Software Ghostscript 10.01.2 版本及之前版本存在安全漏洞，该漏洞源于错误地处理管道设备的权限验证。	重要
CVE-2023-28879	Artifex Software Ghostscript 是美国 Artifex Software 公司的一款开源的 PostScript（一种用于电子产业和桌面出版领域的页面描述语言和编程语言）解析器。该产品可显示 Postscript 文件以及在非 Postscript 打印机上打印 Postscript 文件。\rArtifex Ghostscript 10.01.0 版本及之前版本存在安全漏洞，该漏洞源于存在缓冲区溢出问题，导致内部数据损坏。	严重
CVE-2022-28506	GIFLIB 是一款用于读取和编辑 gif 图像的库。GIFLIB 5.2.1 版本存在安全漏洞，该漏洞源于 gif2rgb.c 的 DumpScreen2RGB()函数存在基于堆的缓冲区溢出。	重要
CVE-2022-39260	Git 是一套免费、开源的分布式版本控制系统。Git 存在安全漏洞，该漏洞源于 Git 错误地处理了某些符号链接。	重要
CVE-2022-23521	Git 是一套免费、开源的分布式版本控制系统。 Git 存在输入验证错误漏洞，该漏洞源于当属性名称超过规定大小时会造成整数溢出。	严重
CVE-2022-41903	Git 是一套免费、开源的分布式版本控制系统。 Git 存在输入验证错误漏洞，该漏洞源于存在整数溢出问题。	严重
CVE-2022-48340	GlusterFS 是 Gluster 公司的 Gluster 的文件系统。 Gluster GlusterFS 11.0 版本存在安全漏洞，该漏洞源于内存释放后重用。	重要
CVE-2023-26253	GlusterFS 是 Gluster 公司的 Gluster 的文件系统。	重要

	Gluster GlusterFS 11.0 版本存在安全漏洞，该漏洞源在 glusterfs/xlators/mount/fuse/src/fuse-bridge.c 中存在堆栈缓冲区溢出。	
CVE-2018-17942	Gnulib 是一个支持多系统运行的 GNU 可移植性库。Gnulib 2018-09-23 之前版本中的 vasnprintf.c 文件的‘convert_to_decimal’函数存在基于堆的缓冲区溢出漏洞，该漏洞源于程序没有执行正确的边界检测。远程攻击者可借助特制的文件利用该漏洞在系统上执行任意代码。	重要
CVE-2020-25969	gnuplot 是一款命令行的交互式工具用户通过输入命令可以将数据资料和数据函数转换为易于观察的平面或立体图形\rgnuplot v5.5 版本存在安全漏洞，该漏洞源于通过函数 plotrequest()包含缓冲区溢出。	严重
CVE-2022-2509	GnuTLS 是一款免费的用于实现 SSL、TLS 和 DTLS 协议的安全通信库。GnuTLS 存在资源管理错误漏洞，该漏洞源于在 gnutls_pkcs7_verify 过程中双倍释放。	重要
CVE-2023-0361	GnuTLS 是一款免费的用于实现 SSL、TLS 和 DTLS 协议的安全通信库。 GnuTLS 存在安全漏洞，该漏洞源于可以通过网络恢复以 RSA 密文加密的密钥。攻击者利用该漏洞可以解密应用程序数据。	重要
CVE-2023-24540	go 是一种富有表现力的、并发的、垃圾收集的通用/系统编程语言。 go 1.20 版本存在安全漏洞，该漏洞源于对 JavaScript 空格处理不当。	重要
CVE-2023-29402	Google Go 是美国谷歌（Google）公司的一种静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。 \rGoogle Go 1.19.10 之前版本、 1.20.0-0 到 1.20.5 版本存在安全漏洞，该漏洞源于使用 cgo 时，go 命令可能会在构建时生成意外代码，这可能会导致意外行为。	严重
CVE-2023-29403	Google Go 是美国谷歌（Google）公司的一种静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。 Google Go 1.19.10 之前版本、1.20.0-0 到 1.20.5 版本存在安全漏洞。攻击者利用该漏洞可以提升权限，从而读取或写入任意内容。	重要
CVE-2023-29404	Google Go 是美国谷歌（Google）公司的一种静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。 Google Go 1.19.10 之前版本、 1.20.0-0 到 1.20.5 版本存在安全漏洞，该漏洞源于使用 cgo 时，go 命令可能会在构建时执行任意代码。	严重
CVE-2023-29405	Google Go 是美国谷歌（Google）公司的一种静态强类型、编译型、并发型，并具有垃圾回收功能的编程语言。 Google Go 1.19.10 之前版本、 1.20.0-0 到 1.20.5 版本存在安全漏洞，该漏洞源于使用 cgo 时，go 命令可能会在构建时执行任意代码。	严重
CVE-2023-39323	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 存在安全漏洞，该漏洞源于行指令（ “//line” ）可用于绕过“//go:cgo_”指令的限制，允许在编译期间传递阻止的链接器和编译器标志,这可能会导致运行 go build 时意外执行任意代码。	重要
CVE-2023-39325	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。	重要
CVE-2023-39326	Google Golang 1.20.10 之前版本、1.21.0 到 1.21.3 版本、http2 v0.17.0 之前版本存在安全漏洞，该漏洞源于快速创建请求并立即重置请求的恶意 HTTP/2 客户端可能会导致服务器资源消耗过多。 Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但	重要

	对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 存在安全漏洞，该漏洞源于恶意 HTTP 发送方可以从请求或响应正文中读取比正文中更多的字节，攻击者利用此漏洞可以导致服务器自动读取大量数据。	
CVE-2022-27664	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。Google Golang 1.18.6 之前版本和 1.19.1 之前的 1.19.x 版本存在安全漏洞，该漏洞源于如果关闭被致命错误抢占，HTTP/2 连接可能会在关闭期间挂起，攻击者可能会导致拒绝服务。	重要
CVE-2022-41715	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。\rGoogle Golang 存在安全漏洞，该漏洞源于 regexp/syntax 限制解析正则表达式时使用的内存。	重要
CVE-2022-2879	Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。\rLinux kernel 5.17.1 之前版本存在竞争条件问题漏洞，该漏洞源于 fs/jbd2/transaction.c 中的 jbd2_journal_wait_updates 具有由 transaction_t 竞争条件导致的 use-after-free。	重要
CVE-2022-41716	由于 unsanitized 空值,恶意攻击者可以在 Windows 上设置环境变量。在系统调用。StartProcess 和 os / exec。Cmd,无效的环境变量值包含空值不正确检查。一个恶意的环境变量值可以利用这种行为为一个不同的环境变量设置一个值。例如,环境变量字符串 A = B x00C = D 设置变量 A = B 和 C = D。	重要
CVE-2022-41723	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。	重要
CVE-2022-41724	Google Golang 存在安全漏洞，该漏洞源于 HPACK 解码器中 CPU 消耗过多，从而导致系统拒绝服务。 Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 存在资源管理错误漏洞。攻击者利用该漏洞导致服务器和客户端在尝试构建响应时死机。	重要
CVE-2022-41725	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。\rGoogle Golang 存在资源管理错误漏洞，该漏洞源于过度资源消耗可能会导致拒绝服务。	重要
CVE-2023-24534	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。	重要

CVE-2023-24536	Google Golang 存在安全漏洞，该漏洞源于 HTTP 和 MIME 标头解析时会分配大量内存，即使在解析小的输入时也是如此，这可能会导致拒绝服务。 Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 存在安全漏洞，该漏洞源于在处理包含大量表单输入时，多部分表单解析会消耗大量 CPU 和内存，攻击者利用该漏洞可以导致拒绝服务。	重要
CVE-2023-24537	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 存在安全漏洞，该漏洞源于在包含行号非常大的//line 指令的 Go 源代码上调用任何 Parse 函数都可能由于整数溢出而导致无限循环。	重要
CVE-2023-45285	Google Golang 是美国谷歌（Google）公司的一种静态强类型、编译型语言。Go 的语法接近 C 语言，但对于变量的声明有所不同。Go 支持垃圾回收功能。Go 的并行模型是以东尼·霍尔的通信顺序进程（CSP）为基础，采取类似模型的其他语言包括 Occam 和 Limbo，但它也具有 Pi 运算的特征，比如通道传输。在 1.8 版本中开放插件（Plugin）的支持，这意味着现在能从 Go 中动态加载部分函数。 Google Golang 1.20.12 之前、go 1.21.0-0 到 1.21.5 版本存在安全漏洞，该漏洞源于如果无法通过安全的 https 和 git+ssh 方式获取模块，则使用 go get 获取带有 .git 后缀的模块可能会回退到不安全的 git 协议。	重要
CVE-2023-4785	gRPC 是 gRPC 开源的一种现代、开源、高性能的远程过程调用 (RPC) 框架。\rgRPC 1.23 版本存在安全漏洞，该漏洞源于 TCP 服务器中缺乏错误处理，允许攻击者通过启动与服务器的大量连接来导致拒绝服务。	重要
CVE-2022-2601	Netgate pfSense CE 是一套免费开源的基于 FreeBSD 的防火墙和路由器软件。\rNetgate pfSense CE 存在安全漏洞，有权更改 NTP GPS 设置的攻击者可能会重写文件系统上的现有文件，导致任意命令执行。	重要
CVE-2022-3775	grub2 是美国 GNU 社区的一款 Linux 系统引导程序。\rgrub2 存在缓冲区错误漏洞，该漏洞源于其字体代码呈现某些 unicode 序列时，它无法正确验证字体的宽度和高度。这些值进一步用于访问字体缓冲区，可能导致越界写入。攻击者可能设计一种能够触发此问题的字体，允许在未经授权的内存段中进行修改，导致数据完整性问题或导致拒绝服务。	重要
CVE-2023-4692	grub2 是美国 GNU 社区的一款 Linux 系统引导程序。\rgrub2 存在安全漏洞，该漏洞源于 NTFS 文件系统驱动程序存在越界写入漏洞。	重要
CVE-2023-25567	GSS-NTLMSSP 是 gssapi 开源的一个实现 NTLM 身份验证的 GSSAPI 库的 mechglue 插件。 GSS-NTLMSSP 1.2.0 之前版本存在缓冲区错误漏洞，该漏洞源于未针对可能触发越界读取的两个元素 av_pair 的长度进行正确检查 ，解码目标信息时可能导致越界读取，攻击者可以通过“gss_accept_sec_context”主入口点触发该漏洞。	重要
CVE-2023-25563	GSS-NTLMSSP 是 gssapi 开源的一个实现 NTLM 身份验证的 GSSAPI 库的 mechglue 插件。 GSS-NTLMSSP 1.2.0 之前版本存在缓冲区错误漏洞，该漏洞源于应用程序允许长度大于 4GB 的令牌，攻击者利用该漏洞可以通过“gss_accept_sec_context”主入口点触发越界读取，解码 NTLM 字段时多次越界读取会触发拒绝服务。	重要
CVE-2023-25565	GSS-NTLMSSP 是 gssapi 开源的一个实现 NTLM 身份验证的 GSSAPI 库的 mechglue 插件。 GSS-NTLMSSP 1.2.0 之前版本存在安全漏洞，该漏洞源于解码目标信息时错误的释放会触发拒绝服	重要

	务，攻击者可以通过“gss_accept_sec_context”主入口点触发该漏洞。	
CVE-2023-25725	2.7.3 之前的 HAProxy 可能允许绕过访问控制，因为 HTTP/1 标头在某些情况下会无意中丢失，也就是“请求走私”。HAProxy 中的 HTTP 标头解析器可以接受空的标头字段名称，这可用于截断 HTTP 标头列表，从而使某些标头在针对 HTTP/1.0 和 HTTP/1.1 进行解析和处理后消失。对于 HTTP/2 和 HTTP/3，影响有限，因为标头在解析和处理之前就消失了，就好像它们不是由客户端发送的一样。固定版本为 2.7.3、2.6.9、2.5.12、2.4.22、2.2.29 和 2.0.31。	严重
CVE-2021-37501	HDFGroup hdf5-h5dump 1.12.0 到 1.13.0 中的缓冲区溢出漏洞允许攻击者通过 /hdf5/tools/lib/h5tools_str.c 中的 h5tools_str_sprint 造成拒绝服务。	重要
CVE-2021-32765	Hiredis 存在安全漏洞，该漏洞允许攻击者提供恶意制作或损坏的 RESP、mult-bulk 协议数据，可导致整数溢出。	重要
CVE-2022-22720	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache HTTP Server 存在环境问题漏洞，该漏洞源于 Apache HTTP Server 在丢弃请求正文时无法关闭入站连接，从而导致请求夹带（request smuggling）。该漏洞影响 Apache HTTP Server 2.4.52 版本及更早版本。	重要
CVE-2022-23943	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache HTTP Server 2.4 版本 2.4.52 和之前版本的 mod_sed 中存在缓冲区错误漏洞，该漏洞允许攻击者使用攻击者提供的数据覆盖堆内存。	重要
CVE-2022-36760	Apache HTTP Server 的 mod_proxy_ajp 中的 HTTP 请求解释不一致(HTTP 请求走私)漏洞允许攻击者将请求走私到其转发请求的 AJP 服务器。此问题影响 Apache HTTP Server Apache HTTP Server 2.4 版本 2.4.54 及以前的版本。	严重
CVE-2006-20001	精心设计的 If:请求头可能会导致在池(堆)内存位置读取或写入一个零字节，超出发送的头值。这可能导致进程崩溃。此问题影响 Apache HTTP Server 2.4.54 及更早版本。	重要
CVE-2023-25690	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。 Apache HTTP Server 2.4.0 版本至 2.4.55 版本存在环境问题漏洞，该漏洞源于某些 mod_proxy 配置允许 HTTP 请求走私攻击。攻击者利用该漏洞可以绕过代理服务器中的访问控制。	严重
CVE-2023-27522	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。 Apache HTTP Server 2.4.30 版本至 2.4.55 版本存在环境问题漏洞，该漏洞源于通过 mod_proxy_uwsgi 发现包含 HTTP 响应走私漏洞。	重要
CVE-2023-31122	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。 Apache HTTP Server 2.4.57 及之前版本存在缓冲区错误漏洞，该漏洞源于 mod_macro 缓冲区存在越界读取漏洞。	重要
CVE-2023-45802	Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。 Apache HTTP Server mod_http2 存在资源管理错误漏洞，该漏洞源于当客户端重置 HTTP/2 流（RST 帧）时，存在一个时间窗口，请求的内存资源不会立即回收。相反，释放被推迟到连接关闭。客户端可以发送新请求并重置，使连接保持繁忙和打开状态，从而导致内存占用持续增长。连接关闭时，所有资源都会被回收，但进程可能会在连接关闭之前耗尽内存。	重要
CVE-2022-29486	Intel Hyperscan 是美国英特尔（Intel）公司的一个高性能的多正则表达式匹配库。	严重

	Intel Hyperscan 2022/4/29 之前版本存在安全漏洞，该漏洞源于对缓冲区限制不当。攻击者利用该漏洞可以升级权限。	
CVE-2022-2068	OpenSSL 是 Openssl 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。OpenSSL 1.0.2、1.1.1 和 3.0 版本存在安全漏洞，该漏洞源于错误地处理了 c_rehash 脚本。本地攻击者可能会在运行 c_rehash 时利用该漏洞执行任意命令。	严重
CVE-2022-0778	在 OpenSSL 中发现一个缺陷。通过制作一个具有无效椭圆曲线参数的证书，可以触发无限循环。由于证书解析发生在验证证书签名之前，因此任何解析外部提供的证书的进程都可能受到拒绝服务攻击。	严重
CVE-2022-1292	OpenSSL 是 Openssl 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。OpenSSL 存在操作系统命令注入漏洞，该漏洞源于 c_rehash 脚本未正确清理 shell 元字符导致命令注入。攻击者利用该漏洞执行任意命令。	严重
CVE-2023-38403	iperf3 是 ESnet 开源的一种用于主动测量 IP 网络上可实现的最大带宽的工具。 iperf3 3.14 之前版本存在安全漏洞。攻击者利用该漏洞通过特制的长度字段导致整数溢出和堆损坏。	重要
CVE-2023-22081	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。 Oracle Java SE 的 Oracle Java SE 8u381 版本，8u381-perf 版本，11.0.20 版本，17.0.8 版本和 20.0.2 版本，Oracle GraalVM for JDK 17.0.8 版本和 20.0.2 版本存在安全漏洞，该漏洞源于允许未经身份验证的攻击者通过 HTTPS 进行网络访问来危害 Oracle Java SE、Oracle GraalVM for JDK。	重要
CVE-2023-21930	Oracle Java SE 和 Oracle GraalVM 都是美国甲骨文（Oracle）公司的产品。Oracle Java SE 是一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle GraalVM 是一套使用 Java 语言编写的即时编译器。该产品支持多种编程语言和执行模式。 Oracle Java SE 8u361、8u361-perf、11.0.18、17.0.6、20 版本, Oracle GraalVM Enterprise 20.3.9、21.3.5 和 22.3.1 版本存在安全漏洞，攻击者利用该漏洞可以对 Oracle Java SE、Oracle GraalVM Enterprise Edition 可访问数据进行未授权访问或完全访问。	重要
CVE-2022-34169	Apache Xalan 是美国阿帕奇（Apache）基金会的开源软件库。 Apache Xalan Java XSLT 库存在输入验证错误漏洞，该漏洞源于在处理恶意的 XSLT 样式表时，存在整数截断问题。这可以用来破坏由内部 XSLTC 编译器生成的 Java 类文件并执行任意的 Java 字节码。 Apache Xalan Java 项目已处于休眠状态并正在退出。预计将来不会有解决这个问题的 Apache Xalan Java 版本。注意：Java 运行时（例如 OpenJDK）包括重新打包的 Xalan 副本。	重要
CVE-2022-21426	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 中存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击者通过多种协议进行网络访问，从而破坏 Oracle Java SE、Oracle GraalVM 企业版。成功攻击此漏洞可能会导致未经授权的能力导致 Oracle Java SE、Oracle GraalVM 企业版的部分拒绝服务（部分 DOS）。	重要
CVE-2022-21443	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 中存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击者通过多种协议进行网络访问，从而破坏 Oracle Java SE、Oracle GraalVM 企业版。成功攻击此漏洞可能会导致未经授权的能力导致 Oracle Java SE、Oracle GraalVM 企业版的部分拒绝服务（部分 DOS）。	重要
CVE-2022-21434	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 中存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击	重要

	者通过多种协议进行网络访问，从而破坏 Oracle Java SE、Oracle GraalVM 企业版。成功攻击此漏洞可导致对部分 Oracle Java SE、Oracle GraalVM 企业版可访问数据进行未经授权的更新、插入或删除访问。	
CVE-2022-21496	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击者通过多种协议进行网络访问，从而破坏 Oracle Java SE、Oracle GraalVM 企业版。成功攻击此漏洞可导致对部分 Oracle Java SE、Oracle GraalVM 企业版可访问数据进行未经授权的更新、插入或删除访问。注意：此漏洞适用于 Java 部署，通常在运行沙盒 Java Web Start 应用程序或沙盒 Java 小程序的客户端中，加载和运行不受信任的代码（例如，来自 Internet 的代码）并依赖 Java 沙盒来确保安全。也可以通过使用指定组件中的 API 来利用此漏洞，例如，通过向 API 提供数据的 Web 服务。	重要
CVE-2022-21476	Oracle Java SE 是美国甲骨文（Oracle）公司的一款用于开发和部署桌面、服务器以及嵌入设备和实时环境中的 Java 应用程序。Oracle Java SE 的 Oracle GraalVM 存在输入验证错误漏洞，该漏洞允许未经身份验证的攻击者通过多种协议进行网络访问，从而破坏 Oracle Java SE、Oracle GraalVM 企业版。成功攻击此漏洞可能导致未经授权访问关键数据或完全访问所有 Oracle Java SE、Oracle GraalVM 企业版可访问数据。注意：此漏洞适用于 Java 部署，通常在运行沙盒 Java Web Start 应用程序或沙盒 Java 小程序的客户端中，加载和运行不受信任的代码（例如，来自 Internet 的代码）并依赖 Java 沙盒来确保安全。也可以通过使用指定组件中的 API 来利用此漏洞，例如，通过向 API 提供数据的 Web 服务。	重要
CVE-2022-2047	Eclipse Jetty 是 Eclipse 基金会的一个开源的、基于 Java 的 Web 服务器和 Java Servlet 容器。Eclipse Jetty 存在安全漏洞，该漏洞源于无效的 URI 解析可能会产生无效的 HttpURI.authority，以下产品和版本受到影响：Eclipse Jetty 9.4.46 及之前版本、10.0.9 及之前版本、11.0.9 及之前版本。	重要
CVE-2022-2048	Eclipse Jetty 是 Eclipse 基金会的一个开源的、基于 Java 的 Web 服务器和 Java Servlet 容器。Eclipse Jetty 存在安全漏洞，该漏洞源于无效的 HTTP/2 请求可能导致拒绝服务，以下产品和版本受到影响：Eclipse Jetty 9.4.46 及之前版本、10.0.9 及之前版本、11.0.9 及之前版本。	重要
CVE-2021-32292	在 ConnMan 中，能够向 gweb 组件发送 HTTP 请求的远程攻击者能够利用 received_data 中基于堆的缓冲区溢出来执行代码。	严重
CVE-2023-1370	netplex json-smart 是开源的一个 JSON Java 解析器。 netplex json-smart 存在安全漏洞，该漏洞源于代码对到达 JSON 输入中的数组或对象的嵌套没有任何限制，嵌套数组和对象的解析是递归完成的，导致堆栈耗尽（堆栈溢出）并导致软件崩溃。	重要
CVE-2022-46663	GNU Less 是美国 GNU 社区的一个应用程序。 GNU Less 609 之前版本存在安全漏洞。攻击者利用该漏洞通过特制数据导致绕过转义序列过滤。	重要
CVE-2022-40320	libConfuse 是 libConfuse 开源的一个用 C 语言编写的配置文件解析器库。libConfuse 3.3 版本存在安全漏洞，该漏洞源于其 confuse.c 组件的 cfg_tilde_expand 存在基于堆的缓冲区越界读取。	重要
CVE-2020-0452	libexif 是一个使用 C 语言编写的函数库。该产品主要用于从图形文件中读写 EXIF 元信息。 libexif 存在输入验证错误漏洞，攻击者可以通过编译器对 libexif 的优化来触发缓冲区溢出，从而触发拒绝服务，并可能运行代码。	重要
CVE-2020-12762	json-c 是一款基于 C 语言的 JSON 解析器。 json-c 0.14 及之前版本中存在输入验证错误漏洞。远程攻击者可借助较大的 JSON 文件利用该漏洞在系统上执行任意代码。	重要
CVE-2022-47629	libksba 是 GnuPG Mirrors 开源的一个使处理 X.509 证书、CMS 数据和相关对象的任务更加容易的库。 libksba 1.6.3 之前版本存在安全漏洞，该漏洞源于在 CRL 签名解析器中容易出现整数溢出漏洞。	严重
CVE-2022-3515	libksba 是 GnuPG Mirrors 开源的一个使处理 X.509 证书、CMS 数据和相关对象的任务更加容易的库。	重要

	libksba 1.3.5-2+deb10u1 版本存在安全漏洞，该漏洞源于 CRL 解析器中存在整数溢出，这可能导致拒绝服务或执行任意代码。	
CVE-2023-26769	Liblouis 是一款使用 C 语言编写的开源的盲文翻译器。 Liblouis v.3.24.0 版本存在安全漏洞，该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 compileTranslationTabel.c 中的 resolveSubtable 函数导致拒绝服务。	重要
CVE-2023-26767	Liblouis 是一款使用 C 语言编写的开源的盲文翻译器。\rLiblouis v.3.24.0 版本存在安全漏洞，该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 logginc.c 端点的 lou_logFile 函数导致拒绝服务。	重要
CVE-2023-26768	Liblouis 是一款使用 C 语言编写的开源的盲文翻译器。\rLiblouis v.3.24.0 版本存在安全漏洞，该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 compileTranslationTable.c 和 lou_setDataPath 函数造成拒绝服务。	重要
CVE-2020-25219	libproxy 是个人开发者的一个提供自动配置代理的库。libproxy 0.4.x 到 0.4.15 版本中存在缓冲区错误漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。	重要
CVE-2021-33643	openEuler 是开放原子开源基金会的一款操作系统。开放原子开源基金会 openEuler 20.03-LTS-SP1，20.03-LTS-SP3 和 22.03-LTS 版本存在安全漏洞，该漏洞源于攻击者如果提交一个头结构中大小为 0 的特制 tar 文件，可能会触发对变量 gnu_longlink 的 malloc(0)调用，从而导致越界读取。	重要
CVE-2021-33645	openEuler 是开放原子开源基金会的一款操作系统。openEuler 20.03-LTS-SP1，20.03-LTS-SP3 和 22.03-LTS 版本存在安全漏洞，该漏洞源于 th_read()函数在分配内存后没有释放变量 t->th_buf.gnu_longlink，这可能会导致内存泄漏。	重要
CVE-2021-33646	openEuler 是开放原子开源基金会的一款操作系统。openEuler 20.03-LTS-SP1，20.03-LTS-SP3 和 22.03-LTS 版本存在安全漏洞，该漏洞源于 th_read()函数在分配内存后没有释放变量 t->th_buf.gnu_longname，这可能会导致内存泄漏。	重要
CVE-2021-46848	Libtasn1 是美国 GNU 社区的一个 GnuTLS、p11-kit 和其他一些软件包使用的 ASN.1 库。\rGNU Libtasn1 4.19.0 之前的版本存在缓冲区错误漏洞，该漏洞源于其 ETYPE_OK 数组大小检查影响 asn1_encode_simple_der。	严重
CVE-2022-3526	Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。Linux kernel 存在安全漏洞。攻击者利用该漏洞导致内存泄漏。	重要
CVE-2022-3570	LibTIFF 是一个读写 TIFF（标签图像文件格式）文件的库。该库包含一些处理 TIFF 文件的命令行工具。LibTIFF 4.4.0 版本存在缓冲区错误漏洞，该漏洞源于存在多个堆缓冲区溢出，允许攻击者通过精心制作的 TIFF 图像文件触发不安全或越界的内存访问，这可能导致应用程序崩溃、潜在的信息泄露或任何其他与上下文相关的影响。	重要
CVE-2023-6277	LibTIFF 是一个读写 TIFF（标签图像文件格式）文件的库。该库包含一些处理 TIFF 文件的命令行工具。 LibTIFF 存在安全漏洞，该漏洞源于内存不足，将精心设计的 tiff 文件传递给 TIFFOpen() API 可能会允许远程攻击者通过大小小于 379 KB 的手工输入造成拒绝服务。	重要
CVE-2020-29260	LibVNCServer 是一款支持在程序中实现 VNC（虚拟网络计算）服务器或客户端功能的跨平台 C 语言库。LibVNCServer libvncclient v0.9.13 版本存在安全漏洞，该漏洞源于函数 rfbClientCleanup()包含一个内存泄漏。	重要
CVE-2023-1999	Mozilla Foundation Security Advisory 将此缺陷描述为： libwebp 中的双重释放可能会导致内存损坏和潜在的可利用崩溃。	严重
CVE-2022-3554	X.Org libX11 是 X.org 基金会的一个 X11（X Window 系统）客户端库。X.org libX11 存在安全漏洞，该	重要

	漏洞源于内存泄漏。	
CVE-2022-4883	libXpm 会调用外部程序来压缩和解压缩文件，依赖于 PATH 环境变量来查找这些程序，这可能允许恶意用户通过操纵 PATH 环境变量来执行其他程序	重要
CVE-2021-30560	Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Chrome 中存在资源管理错误漏洞，该漏洞源于产品的 Blink XSLT 组件中存在对资源释放后仍然使用的缺陷，攻击者可通过诱导用户打开特定网页来引发该漏洞。以下产品及版本受到影响：Google Chrome 70.0.3538.67 至 91.0.4472.124 版本，Microsoft Edge (Chromium-based)。	重要
CVE-2022-47925	Secvisogram 是 Secvisogram 开源的一种网络工具。用于创建和编辑 CSAF 2.0 格式的安全咨询。\rSecvisogram csaf-validator-service 0.1.0 之前版本存在输入验证错误漏洞，该漏洞源于输入验证不充分。攻击者利用该漏洞导致系统拒绝服务。	重要
CVE-2021-2144	Oracle MySQL 的 MySQL 服务器产品中存在漏洞（组件：服务器：解析器）。受影响的支持版本为 5.7.29 及以前版本和 8.0.19 及以前版本。易受攻击的漏洞允许具有网络访问权限的高权限攻击者通过多种协议危害 MySQL 服务器。成功攻击此漏洞可导致接管 MySQL 服务器。CVSS 3.1 基本分数 7.2（保密性、完整性和可用性影响）。CVSS 向量：（CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H）。	重要
CVE-2020-13249	MariaDB 是 MariaDB 基金会的一套免费开源的数据库管理系统，也是一个采用 Maria 存储引擎的 MySQL 分支版本。Connector/C 是其中的一个用于将 C/C++应用程序连接到 MariaDB 和 MySQL 数据库的连接器。MariaDB Connector/C 3.1.8 之前版本中的 libmariadb/mariadb_lib.c 文件存在安全漏洞，该漏洞源于程序没有正确验证从客户端接收到的数据包。目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。	重要
CVE-2020-15180	一个缺陷被发现在 mariadb mysql-wsrep 组件。缺乏输入检查“wsrep_sst_method”允许命令注入,远程攻击者可以利用 galera 集群节点上执行任意命令。这威胁系统的机密性、完整性和可用性。这个缺陷影响 mariadb 10.1.47 之前版本,10.2.34 之前,10.3.25 之前,10.4.15 10.5.6 之前。	重要
CVE-2021-27928	远程代码执行问题被发现在 MariaDB 10.2.37 之前 10.2,10.3 10.3.28 之前,10.4.18 之前 10.4,和 10.5 之前 10.5.9;通过 2021-03-03 Percona 服务器;并通过 2021-03-03 MySQL wsrep 补丁。一个不可信的搜索路径导致 eval 注入,数据库超级用户可以修改 wsrep_provider 和 wsrep_notify_cmd 后执行操作系统命令。注意:这并不影响 Oracle 的产品。	重要
CVE-2022-27385	MariaDB 是 MariaDB（Mariadb）基金会的一套免费开源的数据库管理系统，也是一个采用 Maria 存储引擎的 MySQL 分支版本。MariaDB Server v10.7 及更低版本存在安全漏洞，该漏洞允许攻击者通过特制的 SQL 语句导致拒绝服务 (DoS)。	重要
CVE-2023-5157	MariaDB 是 Mariadb 基金会的一套免费开源的数据库管理系统，也是一个采用 Maria 存储引擎的 MySQL 分支版本。 MariaDB 10.5.21、10.6.14、10.7.7、10.8.6 和 10.9.4 版本存在安全漏洞，该漏洞源于端口 3306 和 4567 上的 OpenVAS 端口允许恶意远程客户端扫描，导致拒绝服务。	重要
CVE-2022-32084	MariaDB 是 Mariadb 基金会的一套免费开源的数据库管理系统，也是一个采用 Maria 存储引擎的 MySQL 分支版本。 该漏洞源于通过组件 sub_select 发现存在分段错误。	重要
CVE-2022-33196	Intel Software Guard Extensions（SGX）是美国英特尔（Intel）公司的一组安全相关的指令，它被内置于一些 Intel 中央处理器中。它提供基于硬件的内存加密，将内存中的特定应用代码和数据隔离开来。Intel(R) Software Guard Extensions 存在安全漏洞，该漏洞源于内存控制器配置中的默认权限不正确。攻击者利用该漏洞可以升级权限。	重要
CVE-2023-23583	Intel Processors（英特尔处理器）是美国英特尔（Intel）公司的提供解释计算机指令以及处理计算机软件中的数据。	重要

	Intel Processors 存在安全漏洞，该漏洞源于处理器指令序列会导致某些英特尔处理器出现意外行为，攻击者利用该漏洞可以通过本地访问实现特权升级、信息泄露或拒绝服务，以下产品和版本受到影响：10th Generation Intel Core Processor Family（Mobile）、3rd Generation Intel Xeon Processor Scalable Family、Intel Xeon D Processor、11th Generation Intel Core Processor Family(Desktop)、1th Generation Intel Core Processor Family(Mobile)、Intel Server Processor。	
CVE-2022-41974	设备映射多路径存在漏洞。设备映射器多路径允许本地用户获得根访问权限，可以单独使用，也可以与 CVE-2022-41973 结合使用。能够写入 UNIX 域套接字的本地用户可以绕过访问控制并操作多路径设置。出现此问题是因为攻击者可以重复关键字，当使用算术 ADD 而不是按位 OR 时，该关键字会被错误处理。这可能导致本地权限升级到根权限。	重要
CVE-2023-29491	ncurses 是一个字符终端处理库，它能够提供一系列函数以供用户调用并生成基于文本的用户界面。ncurses 6.4 20230408 之前版本存在安全漏洞。攻击者利用该漏洞导致内存损坏。	重要
CVE-2023-44487	HTTP/2 是超文本传输协议的第二版，主要用于保证客户机与服务器之间的通信。Apache HTTP/2 存在安全漏洞。攻击者利用该漏洞导致系统拒绝服务。	重要
CVE-2023-35945	Envoy 是一款开源的分布式代理服务器。Envoy 1.27.0 之前版本存在资源管理错误漏洞，该漏洞源于 Envoy 的 HTTP/2 编解码器在收到来自上游服务器的帧 RST_STREAM 后，可能会泄漏 header map 和 bookkeeping structures。	重要
CVE-2021-23017	nginx 解析器被发现安全问题,这可能允许攻击者谁能建立 UDP 数据包从 DNS 服务器造成字节内存覆盖,导致工作进程崩溃或其他潜在的影响。	重要
CVE-2022-40284	在 2022.10.3 之前，NTFS-3G 发现缓冲区溢出。在 NTFS 映像中精心制作的元数据可能导致代码执行。如果 ntfs-3g 二进制文件是 setuid root，本地攻击者就可以利用这一点。如果将 NTFS-3G 软件配置为在连接外部存储设备时执行，那么物理上接近的攻击者就可以利用这一点。	重要
CVE-2022-29155	OpenLDAP 是美国 Openldap 基金会的一个轻型目录访问协议（LDAP）的开源实现。OpenLDAP 2.x 版本至 2.5.12 之前版本、2.6.x 版本至 2.6.2 之前版本存在安全漏洞，该漏洞源于通过 LDAP 查询中的 SQL 语句在 back-sql 后端中存在 SQL 注入漏洞。	严重
CVE-2023-2977	OpenSC 是一款开源的智能卡工具和中间件。OpenSC 存在安全漏洞，该漏洞源于缓冲区溢出，攻击者利用该漏洞可以进行堆的缓冲区越权读取。	重要
CVE-2023-40660	OpenSC 是一款开源的智能卡工具和中间件。OpenSC 0.17.0 到 0.23.0 版本存在安全漏洞，该漏洞源于当令牌卡插入计算机并进行身份验证时，存在潜在的 PIN 绕过。	重要
CVE-2023-38408	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.3p2 之前版本存在安全漏洞，该漏洞源于 ssh-agent 的 PKCS11 功能存在安全问题。攻击者可利用该漏洞执行远程代码。	严重
CVE-2023-51385	OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。	严重
CVE-2023-0464	OpenSSH 9.6 之前版本存在安全漏洞，该漏洞源于存在操作系统命令注入漏洞。在处理证书 policy 校验的时候未做限制，导致遇到恶意证书链时，无法识别。攻击者可以通过创建恶意证书链来利用此漏洞，从而触发计算资源的大量消耗，对系统进行拒绝服务（DOS）攻击。	重要
CVE-2015-8011	lldpd 是一款能够接收和发送 LLDP 帧的守护程序。lldpd 0.8.0 之前版本中的 daemon/protocols/lldp.c 文件中的‘lldp_decode’函数存在缓冲区错误漏洞。远程攻击者可利用该漏洞导致拒绝服务（应用程序	严重

	崩溃）。	
CVE-2020-27827	lldpd 是一款能够接收和发送 LLDP 帧的守护程序。Ubuntu lldpd 软件中存在资源管理错误漏洞，攻击者可利用该漏洞触发拒绝服务攻击。以下产品及型号受到影响：Ubuntu 20.10 openvswitch-common,Ubuntu 20.04 LTS openvswitch-common Ubuntu 18.04 LTS openvswitch-common, Ubuntu 16.04 LTS： openvswitch-common	重要
CVE-2020-35498	Openvswitch 中存在资源管理错误漏洞，该漏洞源于网络系统或产品对系统资源（如内存、磁盘空间、文件等）的管理不当。	重要
CVE-2022-4338	多个版本的 Open vSwitch 容易受到精心设计的 LLDP 攻击，导致拒绝服务和数据下溢攻击的数据包	严重
CVE-2023-1668	Open vSwitch 是一个开源的虚拟交换机。 Open vSwitch 存在安全漏洞，该漏洞源于当处理带有协议 0 的 IP 数据包时，将安装数据路径流，而不对 IP 标头进行修改操作。	重要
CVE-2022-47021	opusfile 是 xiph 开源的一个应用程序。用于解码和查找磁盘上或 http 上的 .ops 文件。 xiph opusfile 0.9 版本至 0.12 版本存在代码问题漏洞，该漏洞源于 opusfile.c 中的函数 op_get_data 和 op_open1 存在空指针取消引用，允许攻击者造成拒绝服务或其他未指定的影响。	重要
CVE-2022-1586	PCRE 是 Philip Hazel 个人开发者的一款使用 C 语言编写的开源正则表达式函数库。 PCRE 存在安全漏洞。攻击者利用该漏洞通过 pcre2_jit_compile.c 中的 compile_xclass_matchingpath 强制读取 PCRE 的无效内存地址，以触发拒绝服务或获取敏感信息。	严重
CVE-2022-1587	PCRE 是 Philip Hazel 个人开发者的一款使用 C 语言编写的开源正则表达式函数库。 PCRE 存在安全漏洞。攻击者利用该漏洞通过 pcre2_jit_compile.c 中的 get_recurse_data_length 强制读取 PCRE 的无效内存地址，以触发拒绝服务或获取敏感信息。	严重
CVE-2021-36770	Perl 是 Perl（PERL）社区的一款通用、解释型、动态的跨平台编程语言。Perl 5 中存在安全漏洞，该漏洞允许攻击者对 Perl5 进程的当前目录具有写访问权从而进行命令执行。	重要
CVE-2023-31486	HTTP::Tiny 是 Perldoc 开源的一个小巧、简单、正确的 HTTP/1.1 客户端。 HTTP::Tiny 存在安全漏洞，该漏洞源于具有不安全的默认 TLS 配置，用户必须选择加入以验证证书。	重要
CVE-2023-31484	2.35 之前的 CPAN.pm 在通过 HTTPS 下载分发版时不验证 TLS 证书。	重要
CVE-2022-44638	Pixman 是一个用于像素操作的低级软件库，提供图像合成和梯形光栅化等功能。Pixman 是一个用于像素操作的低级软件库，提供图像合成和梯形光栅化等功能。 Pixman0.42.2 之前版本的 libpixman 中，由于 Pixman_sample_floor_y 中的整数溢出，rasterize_edges_8 中存在越界写入（也称为基于堆的缓冲区溢出）。	重要
CVE-2023-24056	pkgconf 是 pkgconf 开源的一个帮助为开发库配置编译器和链接器标志的程序。 pkgconf 1.9.3 版本及之前版本存在安全漏洞，该漏洞源于变量重复导致无边界字符串扩展。	严重
CVE-2023-41915	OpenPMIx 是 OpenPMIx 开源的一个 PMIx 标准的 OpenPMIx 实施。\rOpenPMIx PMIx 存在安全漏洞，该漏洞源于允许攻击者在执行 UID 0 的库代码期间获取任意文件的所有权。受影响的产品和版本：OpenPMIx PMIx 4.2.6 之前版本，5.0.1 之前的 5.0.x 版本。	重要
CVE-2020-23804	Freedesktop Poppler 是 Freedesktop 社区的一个用于生成 PDF 的 C++类库，该库是从 Xpdf(PDF 阅读器）继承而来。 Freedesktop Poppler 0.89.0 版本存在安全漏洞。目前尚无此漏洞的相关信息，请随时关注 CNNVD 或厂商公告。	重要
CVE-2021-46854	ProFTPd 是一套可配置性强的开放源代码的 FTP 服务器软件。 ProFTPd 1.3.7c 之前版本存在安全漏洞，该漏洞源于 mod_radius 复制了 16 个字符的块，允许向 RADIUS	重要

	服务器泄露内存。	
CVE-2019-20907	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。Python 3.8.3 版本及之前版本中的 Lib/tarfile.py 文件存在输入验证错误漏洞，该漏洞源于_proc_pax 缺少标头验证。攻击者可借助 TAR 归档文件利用该漏洞导致无限循环。	重要
CVE-2015-20107	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。Python 之前版本存在安全漏洞，该漏洞源于 mailcap 模块不会将转义字符添加到系统 mailcap 文件中发现的命令中。	严重
CVE-2021-28861	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。Python 3.x 系列版本中 3.10 之前版本存在输入验证错误漏洞，该漏洞源于在 lib/http/server.py 中存在一个开放重定向漏洞，因为没有针对 URI 路径开头的多个 (/) 的保护，这可能导致信息泄露。	重要
CVE-2023-24329	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。 Python 3.11 之前版本存在输入验证错误漏洞，该漏洞源于允许攻击者通过提供以空白字符开头的 URL 来绕过黑名单。	重要
	Certifi 是 Certifi 开源的一个 Python SSL 证书。	
CVE-2022-23491	Certifi 2017.11.05 到 2022.12.07 版本存在数据伪造问题漏洞，攻击者利用该漏洞可以从根存储的“TrustCor”中删除根证书。	重要
CVE-2023-37920	Certifi 是 Certifi 开源的一个 Python SSL 证书。 Certifi 2023.07.22 之前版本存在数据伪造问题漏洞，该漏洞源于 e-Tugra 的根证书存在安全漏洞。	重要
CVE-2022-21797	joblib 是 joblib 开源的一组在 Python 中提供轻量级流水线的工具。\rjoblib package 1.2.0 之前的版本存在安全漏洞，该漏洞源于其 Parallel()类中的 pre_dispatch 标志允许攻击者通过 eval()语句实现任意代码执行。	严重
CVE-2022-2309	lxml 是 lxml 个人开发者的一个可与 Python 交互用于定位 Html 中元素的软件。libxml2 是开源的一个用来解析 XML 文档的函数库。它用 C 语言写成，并且能为多种语言所调用，例如 C 语言，C++，XSH。 lxml 和 libxml2 2.9.10 版本至 2.9.14 版本存在代码问题漏洞。攻击者利用该漏洞通过伪造的输入数据触发崩溃。	重要
CVE-2022-45198	9.2.0 之前的 Pillow 对高度压缩的 GIF 数据执行不当处理（数据放大）。	重要
CVE-2022-45199	Pillow before 9.3.0 allows denial of service via SAMPLESPERPIXEL.	重要
	ReportLab 是丹麦 ReportLab 公司的一款用于创建数据驱动的 PDF 文档和自定义矢量图形的开源引擎。	
CVE-2023-33733	Reportlab v3.6.12 及之前版本存在安全漏洞，该漏洞源于允许攻击者通过提供精心制作的 PDF 文件来执行任意代码。	重要
CVE-2022-40897	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。 Python Python Packaging Authority (PyPA) setuptools 65.3.0 版本及之前版本存在安全漏洞。攻击者利用该漏洞通过特制的 HTML 包或自定义 PackageIndex 页面导致拒绝服务。	重要
CVE-2023-25577	python-werkzeug 是一个全面的 WSGI web 应用程序库。在 2.2.3 版本之前，Werkzeug 的多部分表单数据解析器将解析无限数量的部分，包括文件部分。部分可以是少量的字节，但每个部分都需要 CPU 时间来解析，并且可能会使用更多的内存作为 Python 数据。如果可以向访问“request.data”、“request.form”、“request.files”或“request.get_data（parse_form_data=False）”的端点发出请求，则可能会导致意外的高资源使用率。这使得攻击者可以通过将精心编制的多部分数据发送到将对其进行解析的端点来造成拒绝服务。所需的 CPU 时间可能会阻止工作进程处理合法请求。所需的 RAM 数	重要

	量可能会触发进程的内存不足终止。无限的文件部分可能会占用内存和文件句柄。如果连续发送许多并发请求，这可能会耗尽或杀死所有可用的工作者。2.2.3 版包含针对此问题的修补程序。	
CVE-2023-3354	QEMU（Quick Emulator）是法国法布里斯-贝拉（Fabrice Bellard）个人开发者的一套模拟处理器软件。该软件具有速度快、跨平台等特点。 Qemu qemu-kvm 存在安全漏洞，该漏洞源于 TLS handshake 不正确删除会导致拒绝服务（DoS）。	重要
CVE-2020-24165	QEMU（Quick Emulator）是法国法布里斯-贝拉（Fabrice Bellard）个人开发者的一套模拟处理器软件。该软件具有速度快、跨平台等特点。 QEMU 4.2.0 版本存在安全漏洞，该漏洞源于 TCG 加速器存在问题，允许本地攻击者执行任意代码、提升权限并导致拒绝服务(DoS)。	重要
CVE-2022-35414	QEMU（Quick Emulator）是法国法布里斯-贝拉（Fabrice Bellard）个人开发者的一套模拟处理器软件。该软件具有速度快、跨平台等特点。QEMU 的 physmem.c 7.0.0 版本及以下版本存在安全漏洞，该漏洞源于可以对 translate_fail 路径进行未初始化的读取，导致 io_readx 或 io_writex 崩溃。	重要
CVE-2022-1050	Guest 是一个应用产品。Guest 存在资源管理错误漏洞，该漏洞源于当共享缓冲区尚未分配时，Guest driver 会执行 HW 命令，从而导致空闲后使用。	重要
CVE-2023-24607	Qt 是挪威 Qt 公司的一个跨平台的 C++应用程序开发框架。广泛用于开发 GUI 程序，这种情况下又被称为部件工具箱。也可用于开发非 GUI 程序，例如控制台工具和服务器。 Qt 6 存在安全漏洞。攻击者利用该漏洞导致系统拒绝服务。	重要
CVE-2023-32763	Qt 是挪威 Qt 公司的一个跨平台的 C++应用程序开发框架。广泛用于开发 GUI 程序，这种情况下又被称为部件工具箱。也可用于开发非 GUI 程序，例如控制台工具和服务器。 Qt 5.15.15 之前版本、6.2.9 之前的 6.x 版本、6.3.x 至 6.5.1 之前的 6.5.x 版本存在安全漏洞，该漏洞源于存在缓冲区溢出。	重要
CVE-2023-37369	在 5.15.15 之前的 Qt、6.2.9 之前的 6.x 以及 6.5.2 之前的 6.3.x 到 6.5.x 中，QXmlStreamReader 中可能会通过特制的 XML 字符串发生应用程序崩溃，从而触发前缀大于长度的情况。	重要
CVE-2023-38197	在 5.15.15 之前的 Qt、6.2.10 之前的 6.x 以及 6.5.3 之前的 6.3.x 到 6.5.x 中发现了一个问题。递归实体展开中有无限个循环。	重要
CVE-2022-29154	rsync 是 Wayne Davison 个人开发者的一个提供快速增量文件传输的开源实用程序。rsync 3.2.5 之前版本存在安全漏洞，该漏洞源于 rsync 客户端对文件名的验证不足。	重要
CVE-2022-24903	Adiscon Rsyslog 是德国 Adiscon 公司的一个用于收集系统日志的库。Adiscon Rsyslog 之前版本存在安全漏洞，该漏洞源于使用八位字节计数的帧时，用于接收 TCP 系统日志的模块会出现堆缓冲区溢出，攻击者利用该漏洞可以破坏堆值，导致数据完整性和可用性。	重要
CVE-2022-44640	Heimdal 是 Heimdal 开源的一个 Kerberos 的实现及安全程序。 Heimdal KDC 存在安全漏洞，该漏洞源于 ASN.1 编解码器中的无效自由，攻击者利用该漏洞可以使用 Kerberos 进行身份验证可以模拟客户端或服务，规避验证。	重要
CVE-2022-45141	使用 Heimdal 的 Samba AD DC 可以签发 rc4-hmac 加密的 Kerberos 凭据，rc4-hmac 加密很弱，可能会让 HMAC 的保护将被绕过，特权提升。	重要
CVE-2022-38023	samba 有一个缺陷：Netlogon RPC 实现可以使用 rc4-hmac 加密算法，该算法被认为是弱的，即使客户机支持更现代的加密类型，也应该避免使用。这个问题可能允许知道 samba 客户机和服务器之间通信的纯文本内容的攻击者使用相同的 MD5 计算生成数据，并在不被发现的情况下替换它。	重要
CVE-2023-34966	Samba 是用于 Linux 和 Unix 的标准 Windows 互操作性程序套件。 Samba 4.18.5 之前版本存在安全漏洞，该漏洞源于未经身份验证的攻击者可以通过发出格式错误的 RPC 请求来触发无限循环错误。	重要
CVE-2018-0732	OpenSSL 是 OpenSSL 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协	重要

	议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。OpenSSL 1.1.0 版本至 1.1.0h 版本和 1.0.2 版本至 1.0.2o 版本中存在加密问题漏洞。该漏洞源于网络系统或产品未正确使用相关密码算法，导致内容未正确加密、弱加密、明文存储敏感信息等。	
CVE-2020-1971	OpenSSL 是 Openssl 团队的一个开源的能够实现安全套接层（SSLv2/v3）和安全传输层（TLSv1）协议的通用加密库。该产品支持多种加密算法，包括对称密码、哈希算法、安全散列算法等。OpenSSL 1.1.1 版本和 1.0.2 版本存在代码问题漏洞，该漏洞源于空指针解引用和崩溃可能会导致拒绝服务攻击。	重要
CVE-2022-25857	SnakeYAML 是一款基于 Java 的 YAML 解析器。SnakeYAML 1.31 及之前版本存在安全漏洞，该漏洞源于缺少对集合的嵌套深度限制，存在拒绝服务（DoS）问题。	重要
CVE-2023-34454	snappy-java 是 Taro L. Saito 个人开发者的一个压缩程序 snappy 的 java 端口。 snappy-java 1.1.10.1 之前版本存在输入验证错误漏洞，该漏洞源于未检查的乘法运算，可能会发生整数溢出，从而导致致命错误。	重要
CVE-2023-34455	Snappy 是 KNP Labs 个人开发者的一个 PHP 库，允许从 url 或 html 页面生成缩略图、快照或 PDF。Snappy snappy-java 1.1.10.1 之前版本存在输入验证错误漏洞，该漏洞源于未检查的乘法运算，可能会发生整数溢出，从而导致致命错误。	重要
CVE-2023-43642	Snappy 是 KNP Labs 个人开发者的一个 PHP 库，允许从 url 或 html 页面生成缩略图、快照或 PDF。Snappy 1.1.10.3 及之前版本存在安全漏洞，该漏洞源于 SnappyInputStream 缺少对块长度的上限检查，导致解压过大的数据时容易受到拒绝服务（DoS）攻击。	重要
CVE-2023-34432	SoX 是一套开源的音频处理工具。该产品支持播放、转换和录制多种格式音频。\rsox 存在安全漏洞，该漏洞源于 sx_readbuf 函数（位于 sox/src/formats_i.c:98:16）中发现堆缓冲区溢出问题，可能会导致拒绝服务、代码执行或信息泄露。	重要
CVE-2023-34318	SoX 是一套开源的音频处理工具。该产品支持播放、转换和录制多种格式音频。\rSoX 存在安全漏洞，该漏洞源于在 startread 函数中存在堆缓冲区溢出漏洞，可能导致拒绝服务、代码执行或信息泄露。	重要
CVE-2023-32697	SQLite 是一款轻型的数据库，是遵守 ACID 的关系型数据库管理系统。\rSQLite JDBC 3.6.14.1 到 3.41.2.1 版本存在代码注入漏洞，该漏洞源于远程代码执行漏洞。	严重
CVE-2021-46784	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。Squid 多个版本存在安全漏洞，该漏洞源于应用存在处理 Gopher 服务器响应时的可访问断言。	重要
CVE-2022-41318	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。Squid 存在安全漏洞。攻击者利用该漏洞可以通过 SSPI / SMB 身份验证强制读取 Squid 缓存的无效内存地址，以触发拒绝服务或获取敏感信息。	重要
CVE-2023-46846	由于块解码器的宽容，Squid 在解析 HTTP/1.1 和 ICAP 消息时容易受到请求/响应走私攻击。	重要
CVE-2023-46847	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。 Squid 6.4 之前版本存在安全漏洞，该漏洞源于缓冲区溢出，容易受到 HTTP 服务攻击。	严重
CVE-2023-46724	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。 Squid 6.4 之前版本存在安全漏洞，该漏洞源于指定索引错误验证不正确，容易受到针对 SSL 证书验证的拒绝服务攻击。	重要
CVE-2023-46728	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。 Squid 6.0.1 之前版本存在代码问题漏洞，该漏洞源于 NULL 指针取消引用，从而导致系统拒绝服务。	重要
CVE-2023-49285	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。	重要

	Squid 存在安全漏洞，该漏洞源于缓冲区溢出错误，从而导致拒绝服务。	
CVE-2023-49286	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。 Squid 6.5 之前版本存在安全漏洞，该漏洞源于函数返回值错误检查不正确，容易受到拒绝服务攻击。	重要
CVE-2023-50269	Squid 是一套代理服务器和 Web 缓存服务器软件。该软件提供缓存万维网、过滤流量、代理上网等功能。 Squid 2.6 到 2.7.STABLE9、3.1 到 5.9 、6.0.1 到 6.5 版本存在安全漏洞，该漏洞源于系统存在不受控制的递归错误，在配置 follow_x_forwarded_for 功能后，允许远程客户端通过发送大型 X-Forwarded-For 标头来执行拒绝服务攻击。	重要
CVE-2023-42465	Sudo 是一款使用于类 Unix 系统的，允许用户通过安全的方式使用特殊的权限执行命令的程序。 Sudo 1.9.15 之前版本存在安全漏洞，该漏洞源于容易受到 ROWHAMMER 攻击，可以绕过 SUDO 身份验证。	重要
CVE-2022-43995	Sudo 1.8.0 至 1.9.12，带有加密（ ）密码后端，包含一个插件/sudoers/auth/passwd.c 数组越界错误，该错误可能导致基于堆的缓冲区过度读取。这可以由具有 Sudo 访问权限的任意本地用户通过输入 7 个字符或更少字符的密码来触发。影响可能因系统库、编译器和处理器体系结构而异。	重要
CVE-2023-22809	Sudo 是一个用于类 Unix 计算机操作系统的程序，它能够使用户能够以另一个用户（默认是超级用户）的安全权限运行程序。sudoedit 功能用于以另外一个用户身份编辑文件。	重要
CVE-2023-33204	sysstat 是一套适用于 Linux 平台的系统性能监控工具。 sysstat 12.7.2 及之前版本存在安全漏洞，该漏洞源于 common.c 中的 check_overflow 存在乘法整数溢出。	重要
CVE-2021-35331	Tcl 是一个免费可用的开源包。提供了一个强大的平台，用于创建将各种应用程序、协议、设备和框架联系在一起的集成应用程序。Tcl 8.6.11 版本存在格式化字符串错误漏洞，该漏洞源于程序的 nmakehlp.c 中的格式字符串漏洞可能允许通过 crated 文件执行代码。	重要
CVE-2023-32700	LuaTeX 是 LuaTeX 公司的 pdfTeX 的扩展版本，使用 Lua 作为嵌入式脚本语言。 LuaTeX 1.17.0 之前版本存在安全漏洞，该漏洞源于在编译从不受信任来源获得的 TeX 文件时允许执行任意 shell 命令。	重要
CVE-2023-1393	X.org Server 是 X.org 基金会的一个开放源代码的自由软件。 X.Org Server 存在安全漏洞，该漏洞源于存在释放后重用，可能会导致本地特权升级。	重要
CVE-2023-1108	由于 SslConduit 中更新了意外的握手状态，因此此问题使得实现拒绝服务成为可能，其中循环从未终止。	重要
CVE-2023-2609	9.0.1531 之前的 vim 中的 NULL 指针取消引用。	重要
CVE-2023-2610	9.0.1532 之前的 vim 中的整数溢出或 Wraparound。	重要
CVE-2023-1170	Vim 是一款跨平台的文本编辑器。 Vim 9.0.1376 之前版本存在安全漏洞，该漏洞源于存在基于堆的缓冲区溢出的问题。	重要
CVE-2023-0433	Vim 是一款跨平台的文本编辑器。 vim/vim 9.0.1225 之前版本存在安全漏洞，该漏洞源于基于堆的缓冲区溢出。	重要
CVE-2022-47024	Vim 是一款跨平台的文本编辑器。 vim 8.1.2269 版本至 9.0.0339 版本存在代码问题漏洞，该漏洞源于 gui_x11.c 中的函数 gui_x11_create_blank_mouse 中存在空指针取消引用，允许攻击者造成拒绝服务或其他未指定的影响。	重要
CVE-2023-0288	Vim 是一款跨平台的文本编辑器。 vim/vim 9.0.1189 之前的版本存在安全漏洞，该漏洞源于攻击者可以实现基于堆的缓冲区溢出。	重要
CVE-2023-0049	Vim 是一款跨平台的文本编辑器。 Vim 9.0.1143 之前版本存在缓冲区错误漏洞，该漏洞源于存在越界读取问题。	重要

CVE-2023-0051	Vim 是一款跨平台的文本编辑器。 Vim 9.0.1144 之前版本存在安全漏洞，该漏洞源于存在基于堆的缓冲区溢出漏洞。	重要
CVE-2023-0054	Vim 是一款跨平台的文本编辑器。 Vim 9.0.1145 之前版本存在缓冲区错误漏洞，该漏洞源于存在越界写入问题。	重要
CVE-2022-4292	Vim 是一款跨平台的文本编辑器。 Vim 9.0.0882 之前版本存在安全漏洞，该漏洞源于存在释放后重用。	重要
CVE-2022-3491	Vim 是一款跨平台的文本编辑器。 Vim 9.0.0742 之前版本存在安全漏洞，该漏洞源于包含堆的缓冲区溢出问题。	严重
CVE-2022-3591	Vim 是一款跨平台的文本编辑器。 Vim 9.0.0789 之前版本存在安全漏洞，该漏洞源于包含释放后重用问题。	重要
CVE-2022-0135	virglrenderer 是一款 VirGL 虚拟 OpenGL 渲染器。Virglrenderer 中存在缓冲区错误漏洞，该漏洞源于产品的 read_transfer_data 函数未能正确处理内存边界。攻击者可通过该漏洞触发拒绝服务，并可能运行代码。	重要
CVE-2022-4283	在 X.Org 中发现一个漏洞。发生此安全漏洞是因为 XkbCopyNames 函数留下了一个指向已释放内存的悬空指针，导致后续 XkbGetKbdByName 请求访问内存超出限制。此问题可能导致 X 服务器运行特权的系统上的本地特权提升，并导致 ssh X 转发会话的远程代码执行。	重要
CVE-2022-46340	在 X.Org 中发现一个漏洞。如果通过 XTestFakeInput 请求发送长度大于 32 字节的 GenericEvents，则 XTest 扩展的 XTestFakeInput 请求的交换处理程序可能会破坏堆栈，因此会出现此安全缺陷。此问题可能导致 X 服务器运行特权的系统上的本地特权提升，并导致 ssh X 转发会话的远程代码执行。此问题不会影响客户端和服务器使用相同字节顺序的系统。	重要
CVE-2022-46341	在 X.Org 中发现一个漏洞。出现此安全缺陷的原因是，当使用高键码或按钮代码调用 XIPassiveUngrab 请求的处理程序时，该处理程序访问了超出边界的内存。此问题可能导致 X 服务器运行特权的系统上的本地特权提升，并导致 ssh X 转发会话的远程代码执行。	重要
CVE-2022-46342	在 X.Org 中发现一个漏洞。出现此安全缺陷是因为 XvdiSelectVideoNotify 请求的处理程序可能在释放请求后写入内存。	重要
CVE-2022-46343	在 X.Org 中发现一个漏洞。出现此安全缺陷是因为 ScreenSaverSetAttributes 请求的处理程序在释放请求后可能会写入内存。此问题可能导致 X 服务器运行特权的系统上的本地特权提升，并导致 ssh X 转发会话的远程代码执行	重要
CVE-2022-46344	在 X.Org 中发现一个漏洞。出现此安全缺陷是因为 XIChangeProperty 请求的处理程序存在长度验证问题，导致超出边界的内存读取和潜在的信息泄露。此问题可能导致 X 服务器运行特权的系统上的本地特权提升，并导致 ssh X 转发会话的远程代码执行	重要
CVE-2023-0494	在 X.Org 中存在漏洞。发生此问题的原因是 DeepCopyPointerClasses 中的一个悬空指针，ProcXkbSetDeviceInfo（ ）和 ProcXkbGetDeviceInfo（ （ ）可以利用该指针读取和写入释放的内存。这可能会导致 X 服务器为 ssh X 转发会话运行特权和远程代码执行的系统上的本地权限提升。	重要
CVE-2022-3550	X.org Server 是 X.org 基金会的一个开放源代码的自由软件。X.org Server 存在安全漏洞，该漏洞源于存在缓冲区溢出漏洞。	重要
CVE-2023-5367	xorg-x11-server 是 X.org 基金会的一款 X 窗口系统显示服务器。 xorg-x11-server 存在安全漏洞，该漏洞源于缓冲区偏移量计算不正确。攻击者利用该漏洞导致权限升级或拒绝服务。	重要
CVE-2023-6478	xorg-x11-server 是 X.org 基金会的一款 X 窗口系统显示服务器。 xorg-server 21.1.10 之前版本、xwayland 23.2.3 之前版本存在安全漏洞，该漏洞源于对 RRChangeProviderProperty 或 RRChangeOutputProperty 的特制请求可能会触发整数溢出，从而导致敏	重要

	感信息泄露。	
CVE-2023-6377	xorg-x11-server 是 X.org 基金会的一款 X 窗口系统显示服务器。 xorg-server 21.1.10 之前版本、xwayland 23.2.3 之前版本存在安全漏洞，该漏洞源于通过查询或更改 XKB 按钮操作可能会导致内存读写越界，在涉及 X11 转发的情况下，这可能允许本地权限升级或可能的远程代码执行。	重要
CVE-2022-24795	yajl-ruby 是美国 Brian Lopez 个人开发者的一个 Ruby 的流式 JSON 解析和编码库。yajl-ruby 存在安全漏洞，该漏洞源于在处理大于 2GB 的输入时会导致堆内存损坏。	重要
CVE-2022-3625	Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。Linux Kernel 存在资源管理错误漏洞，该漏洞源于组件 IPsec 中 net/core/devlink.c 文件的 devlink_param_set/devlink_param_get 函数存在问题，可能导致释放后重用。	重要
CVE-2020-35728	FasterXML jackson-databind 是一个基于 JAVA 可以将 XML 和 JSON 等数据格式与 JAVA 对象进行转换的库。Jackson 可以轻松的将 Java 对象转换成 json 对象和 xml 文档，同样也可以将 json、xml 转换成 Java 对象。FasterXML jackson-databind 2.x 版本至 2.9.10.8 版本存在代码问题漏洞，该漏洞源于错误地处理了序列化小工具和类型之间的交互，涉及到 com.oracle.wls.shaded.org.apache.xalan.lib.sql.JNDIConnectionPool (aka embedded Xalan in org.glassfish.web/javax.servlet.jsp.jstl)。	重要
CVE-2022-41853	HSQLDB 是 The HSQL Development Group 团队的一个用 Java 编写的关系数据库管理系统。HSQLDB 存在安全漏洞，该漏洞源于其使用 java.sql.Statement 或 java.sql.PreparedStatement 处理不可信输入时，默认情况下允许调用类路径中任何 Java 类的任何静态方法，导致攻击者可以执行代码。	重要
CVE-2022-4603	ppp 是 Paul PPP Package 开源的一个实现点对点协议（ppp）的库。 ppp 存在缓冲区错误漏洞，该漏洞源于 pppdump 组件中 pppdump/pppdump.c 文件的 dumpppp 函数存在问题，对参数 spkt.buf/rpkt.buf 的操作会导致数组索引的验证不正确。	重要
CVE-2022-41953	Git 是一套免费、开源的分布式版本控制系统。 Git GUI 存在代码问题漏洞，该漏洞源于 Tcl 脚本在 Windows 上的危险设计，导致在查找可执行文件时的搜索路径始终包括当前目录。	重要
CVE-2022-48303	GNU Tar 是美国 GNU 社区的一套用于创建 tar 格式文件的工具。 GNU Tar 1.34 及之前版本存在安全漏洞，该漏洞源于存在一个单字节越界读取，导致使用未初始化的内存进行条件跳转。	重要
CVE-2023-28708	Apache Tomcat 是美国阿帕奇（Apache）基金会的一款轻量级 Web 应用服务器。该程序实现了对 Servlet 和 JavaServer Page（JSP）的支持。 Apache Tomcat 存在安全漏洞，该漏洞源于用户代理能通过不安全的通道传输会话 cookie 导致信息泄露。以下产品和版本收到影响： Apache Tomcat 11.0.0-M1 至 11.0.0-M2 版本， Apache Tomcat 10.1.0-M1 至 10.1.5 版本， Apache Tomcat 9.0.0-M1 至 9.0.71 版本， Apache Tomcat 8.5.0 至 8.5.85 版本。	重要
CVE-2023-29007	Git 是一套免费、开源的分布式版本控制系统。 Git 存在注入漏洞。攻击者利用该漏洞可以远程执行代码。	重要
CVE-2023-25652	Git 是一套免费、开源的分布式版本控制系统。 Git 存在路径遍历漏洞。攻击者利用该漏洞可以访问存储在 web 根文件夹之外的文件和目录。以下版本受到影响：2.30.9 版本、2.31.8 版本、2.32.7 版本、2.33.8 版本、2.34.8 版本、2.35.8 版本、2.36.6 版本、2.37.7 版本、2.38.5 版本、2.39.3 版本、2.40.1 版本。	重要

CVE-2023-30570	Libreswan 是一个类似于 Openswan 的 IPsec 实现，它主要用于保证数据传输中的安全性、完整性问题。Libreswan 存在安全漏洞。攻击者利用该漏洞通过虚拟专用网络(VPN)等不受信任的网络构建安全隧道。	重要
CVE-2022-1941	Google protobuf 是美国谷歌（Google）公司的一种数据交换格式。Google protobuf protobuf-cpp 和 protobuf-python 存在缓冲区错误漏洞，该漏洞源于在处理特制消息时触发内存不足 (OOM) 故障，从而导致拒绝服务。以下产品及版本受到影响：protobuf-cpp 3.16.1 版本及之前版本、3.17.3 版本及之前版本、3.18.2 版本及之前版本、3.19.4 版本及之前版本、3.20.1 版本及之前版本、3.21.5 版本及之前版本，protobuf-python 3.16.1 版本及之前版本、3.17.3 版本及之前版本、3.18.2 版本及之前版本、3.19.4 版本及之前版本、3.20.1 版本及之前版本、4.21.5 版本及之前版本。	重要
CVE-2023-30861	Pallets Project Flask 是 Pallets 项目的一款轻量级的 WSGI（Web 服务器网关接口）应用程序框架。Flask 存在安全漏洞，该漏洞源于用于一个客户端的数据响应可能会被缓存并随后由代理发送给其他客户端。	重要
CVE-2022-48565	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。Python 3.9.1 存在安全漏洞，该漏洞源于存在 XML 外部实体问题。	严重
CVE-2022-48566	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。Python 3.9.1 存在安全漏洞，该漏洞源于 Lib/hmac.py 的 Compare_digest 累加器变量可以实现恒定时间优化。	重要
CVE-2022-48174	BusyBox 是乌克兰 Denis Vlasenko 个人开发者的一套包含了多个 linux 命令和工具的应用程序。BusyBox 存在安全漏洞，该漏洞源于 ash.c:6030 存在堆栈溢出漏洞。	重要
CVE-2023-40589	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。FreeRDP 存在安全漏洞，该漏洞源于 ncrush_decompress 函数中存在全局缓冲区溢出。向此函数提供精心设计的输入可能会触发溢出，而这仅被证明会导致崩溃。	重要
CVE-2023-39354	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。FreeRDP 存在缓冲区错误漏洞，该漏洞源于 nsc_rle_decompress_data 函数中处理 `context->Planes` 时没有检查它是否包含足够长度的数据。	重要
CVE-2023-39351	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。FreeRDP 存在代码问题漏洞，该漏洞源于在某些特殊情况下，tiles 的初始化过程没有完成，tiles 将会有一个 NULL 指针。将会导致空指针取消引用。	重要
CVE-2023-39350	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。FreeRDP 存在数字错误漏洞，该漏洞源于当提供的 blockLen 不足且未执行适当的长度验证时，会发生整数下溢，从而导致拒绝服务 (DOS) 漏洞。	重要
CVE-2023-23918	Node.js < 19.6.1 、 < 18.14.1 、 < 16.19.1 和 < 14.21.3 中存在权限提升漏洞，可以绕过实验权限(https://nodejs.org/api/permissions.html)特性，并使用 process.mainModule.require（）访问未授权的模块。这只影响使用--experimental 策略启用了实验权限选项的用户。	重要
CVE-2023-30581	在 Node.js 中发现了一个漏洞，在 process.mainModule.proto.require（）中使用 proto 可以绕过策略机制，需要 policy.json 定义之外的模块。	重要
CVE-2023-32006	使用`module.constructor.createRequire（）`可以绕过策略机制，并为给定模块要求 policy.json 定义之外的模块。此漏洞影响所有活动发布行中使用实验策略机制的所有用户：16.x、18.x 和 20.x。请注意，在发布此 CVE 时，该策略是 Node.js 的实验功能	重要
CVE-2023-32002	`Module 的使用_load（）`可以绕过策略机制，并要求给定模块使用 policy.json 定义之外的模块。此漏	严重

	洞影响所有活动发布行中使用实验策略机制的所有用户：16.x、18.x 和 20.x。请注意，在发布此 CVE 时，该策略是 Node.js 的实验功能。	
CVE-2023-3823	在 8.0.30 之前的 8.0.*、8.1.22 之前的 8.1.*和 8.2.8 之前的 8.2.*版本中，各种 XML 函数都依赖于 libxml 全局状态来跟踪配置变量，比如是否加载了外部实体。除非用户通过调用适当的函数显式地更改此状态，否则假定此状态不变。然而，由于状态是进程全局的，其他模块（如 ImageMagick）也可以在同一进程中使用此库，并出于内部目的更改该全局状态，并使其处于启用外部实体加载的状态。这可能导致在加载外部实体的情况下解析外部 XML，从而导致 PHP 可访问的任何本地文件被泄露。这种易受攻击的状态可能会在多个请求的同一进程中持续存在，直到进程关闭。	重要
CVE-2023-3824	在 8.0.30 之前的 PHP 8.0.*版本、8.1.22 之前的 8.1.*版本和 8.2.8 之前的 8.2.*版本中，在加载 phar 文件时，在读取 phar 目录项时，长度检查不足可能会导致堆栈缓冲区溢出，从而可能导致内存损坏或 RCE。	严重
CVE-2023-0662	在 PHP 8.0.28 之前的 8.0.X、8.1.16 之前的 8.1.X 和 8.2.3 之前的 8.2.X 中，HTTP 表单上传中的部分数量过多会导致资源消耗和日志条目数量过多。这可能会耗尽 CPU 资源或磁盘空间，从而导致受影响服务器上的服务被拒绝。	重要
CVE-2023-40217	Python 是 Python 基金会的一套开源的、面向对象的程序设计语言。该语言具有可扩展、支持模块和包、支持多种平台等特点。 Python 存在安全漏洞，该漏洞源于在某种情况下使用 socket 可以造成信息泄露。	重要
CVE-2023-28450	dnsmasq 是一款使用 C 语言编写的轻量级 DNS 转发和 DHCP、TFTP 服务器。 dnsmasq 2.90 之前版本存在安全漏洞，该漏洞源于 EDNS.0 UDP 数据包大小设置为 4096，但实际大小应为 1232。	重要
CVE-2023-4738	vim 中存在基于堆的缓冲区溢出型安全漏洞。	重要
CVE-2023-4752	在 Vim 中发现了一个缺陷，在 ins_compl_get_exp 函数中释放后很容易被使用。此缺陷允许特制的文件在 Vim 中打开时使软件崩溃、使用意外值或可能执行代码。	重要
CVE-2023-4750	在 vim 中存在释放后使用漏洞.	重要
CVE-2023-4733	vim 中存在释放后重用安全漏洞。	重要
CVE-2023-4736	vim 中存在不受信任的搜索路径。	重要
CVE-2023-4735	在 vim 中存在越界写入安全漏洞	重要
CVE-2023-4734	vim 中的整数溢出或 Wraparound。	重要
CVE-2023-4781	vim 中存在基于堆的缓冲区溢出安全漏洞。	严重
CVE-2023-5344	vim 中存在基于堆的缓冲区溢出安全漏洞。	重要
CVE-2023-5535	vim 存在释放后重用安全漏洞。	重要
CVE-2023-30589	Node v220.2.0 中 http 模块中的 llhttp 解析器没有严格使用 CRLF 序列来分隔 http 请求。这可能导致 HTTP 请求走私（HRS）。CR 字符（不带 LF）足以在 llhttp 解析器中分隔 HTTP 头字段。根据 RFC7230 第 3 节，只有 CRLF 序列应该对每个报头字段进行定界。这会影响所有 Node.js 活动版本：v16、v18 和 v20	重要
CVE-2022-40151	那些使用 Xstream 对 XML 数据进行序列化的用户可能容易受到拒绝服务攻击（DOS）的攻击。如果解析器是在用户提供的输入上运行的，则攻击者可能会提供导致解析器崩溃的内容。这种影响可能支持拒绝服务攻击。	重要
CVE-2023-44442	在 GNU 映像操作程序（GIMP）中发现解析漏洞。此漏洞允许未经身份验证的远程攻击者诱骗 GIMP 用户打开恶意 PSD 文件，从而可能在 GIMP 进程中执行未经授权的代码	重要
CVE-2023-44444	在 GNU 映像操作程序（GIMP）中发现解析漏洞。此漏洞允许未经身份验证的远程攻击者诱骗 GIMP 用户打开恶意 PSP 文件，从而可能在 GIMP 进程中执行未经授权的代码。	重要

CVE-2022-41966	XStream 将 Java 对象序列化为 XML，然后再序列化。1.4.20 之前的版本可能允许远程攻击者通过堆栈溢出错误终止应用程序，从而导致仅通过操作已处理的输入流来拒绝服务。该攻击使用集合和映射的哈希代码实现来强制递归哈希计算，从而导致堆栈溢出。此问题在 1.4.20 版本中进行了修补，该版本处理堆栈溢出并引发 InputManipulationException。对于只使用 HashMap 或 HashSet 并且 XML 仅将其作为默认映射或集合引用的用户，一个潜在的解决方法是根据引用的咨询中的代码示例更改 java.util.map 和 java.util 的默认实现。但是，这意味着您的应用程序不关心映射的实现，并且所有元素都是可比较的。	重要
CVE-2022-4065	在 cbeust testng 7.5.0/7.6.0/7.6.1/7.7.0 中发现了一个漏洞。它已被宣布为关键。受此漏洞影响的是组件 XML 文件分析器的 testng core/src/main/java.org/testng/JarFileUtils.java 文件的函数 testngXmlExistsInJar。该操作导致路径遍历。可以远程发起攻击。升级到 7.5.1 和 7.7.1 版本可以解决这个问题。	重要
CVE-2024-23301	在 2.7 之前的 Relax and Recover（ReaR）中发现了一个缺陷，该缺陷在使用 GRUB_RESCUE=y 时创建了一个全局可读的 initrd。此问题可能允许本地攻击者访问系统机密，否则只能由 root 用户读取。	重要
CVE-2023-35887	Apache MINA 是美国阿帕奇（Apache）基金会的一款网络应用程序框架。该产品主要用于开发高性能和高可伸缩性的网络应用程序。 Apache MINA 1.0 版本至 2.10 之前版本存在路径遍历漏洞，该漏洞源于存在未经授权的敏感信息泄露。	重要
CVE-2022-26592	LibSass 是一个开源的使用 C 语言编写的 Sass（CSS 扩展语言）解析器。 LibSass 3.6.5 版本存在安全漏洞，该漏洞源于 CompoundSelector::has_real_parent_ref 函数产生的堆栈溢出漏洞。	重要
CVE-2022-43358	LibSass 是一个开源的使用 C 语言编写的 Sass（CSS 扩展语言）解析器。 LibSass 3.6.5 版本存在安全漏洞，该漏洞源于 ComplexSelector::has_placeholder 存在拒绝服务 (DoS) 漏洞。	重要
CVE-2022-43357	LibSass 是一个开源的使用 C 语言编写的 Sass（CSS 扩展语言）解析器。 LibSass 3.6.5 版本存在安全漏洞，该漏洞源于 CompoundSelector::has_real_parent_ref 中的 ast_selectors.cpp 中存在堆栈溢出漏洞。	重要
CVE-2021-33391	HTACG HTML Tidy 是 HTML Tidy Advocacy Community Group 开源的一个 HTML 工具。 HTACG HTML Tidy v5.7.28 版本存在安全漏洞，该漏洞源于允许攻击者通过 gdoc.c 中 CleanNode() 函数的 -g 选项执行任意代码。	严重
CVE-2022-40023	SQLAlchemy 是一款基于 Python 的开源数据库 ORM 软件。该产品主要提供 SQL 工具包及对象关系映射工具。 SQLAlchemy mako 1.2.2 之前版本存在安全漏洞，该漏洞源于在使用 Lexer 类进行解析时容易受到正则表达式拒绝服务的攻击。	重要
CVE-2023-50229	BlueZ Phone Book 访问配置文件存在基于堆的缓冲区溢出漏洞，允许远程代码执行。	重要
CVE-2024-22211	FreeRDP 是 FreeRDP 团队的一款开源的远程桌面协议（RDP）的实现。 FreeRDP 存在安全漏洞，该漏洞源于“freerdp_bitmap_planar_context_reset”中的整数溢出会导致堆缓冲区溢出。	重要
CVE-2023-36328	libtommath 是 libtom 开源的一个完全用 C 编写的免费开源可移植数论多精度整数 (MPI) 库。 libtommath beba892bc0d4e4ded4d667ab1d2a94f4d75109a9 之前版本存在安全漏洞，该漏洞源于 mp_grow 中存在整数溢出，允许攻击者执行任意代码并导致拒绝服务 (DoS)。	严重
CVE-2024-24806	libuv 是一个 nodejs 的跨平台异步 IO 库。该平台用于抽象 Windows 的 IOCP 及 Unix 的 libev。目前支持的特性有非阻塞;TCP 套接字 ;非阻塞命名管道 ;UDP; 定时器 ;子进程生成;实现异步 DNS ;异步文件系统; 正在运行程序路径查找; 线程池调度; TTY 控制的 ANSI 转义代码; 文件系统事件; 进程间的 IPC 与套接字共享。	重要

CVE-2024-24577	libuv 1.48.0 之前版本存在代码问题漏洞，该漏洞源于允许攻击者制作解析为非预期 IP 地址的有效载荷，从而绕过开发人员检查，可能会受到服务器端请求伪造(SSRF)攻击。 libgit2 是 Git 核心方法的可移植 C 实现，作为一个具有坚实 API 的可链接库提供，允许在应用程序中构建 Git 功能。对“git_index_add”使用精心编制的输入可能会导致堆损坏，而堆损坏可用于执行任意代码。“src/libgit2/index.c”中的“has_dir_name”函数存在问题，该函数释放了一个不应释放的条目。释放的条目稍后会被使用，并被潜在的不良参与者控制的数据覆盖，从而导致受控堆损坏。根据使用 libgit2 的应用程序的不同，这可能导致任意代码的执行。此问题已在 1.6.5 和 1.7.2 版本中进行了修补。	重要
CVE-2023-3966	Open vSwitch 是一个开源的虚拟交换机。 Open vSwitch 存在安全漏洞。攻击者利用该漏洞导致拒绝服务和无效的内存访问。	重要

7. 附录 3 内核问题修复

- 修复 bpf psock kcm/tls 潜在的越界访问问题
- 禁止使用 ptrace 接口跟踪 init 1 程序
- 修复 pipe 驱动优化导致 ovs 某些情况下进程没有被唤醒的问题
- 修复 epoll 在 nonblock 模式下，某些错误路径下引用计数不正确导致内存泄露问题
- 修复文件系统在日志记录和同步之间潜在的竞态条件导致数据丢失的问题
- 修复 S2500 的网卡自适应优化程序导致某些情况下内核崩溃的问题
- 修复 dm-thin-pool 数据提交失败可能触发 UAF 的问题
- 修复 perf event 子系统潜在的 Use-After-Free 的问题
- 修复 __skb_gso_segment 潜在的内核崩溃问题
- 修复 AMDGPU debugfs 接口存在的空指针引用问题
- 修复 nvmet 自测程序报告的内核崩溃问题
- 修复飞腾架构虚拟机 vcpu 为 0 的 dcache 清理问题
- 修复 Loongarch KVM vcpu timer 问题

- 修复 padata 存在的 UAF 崩溃问题
- 修复 ext4 文件系统在 IO 错误的情况下导致 quota 数据不一致的问题
- 修复 dm-thin-pool kworker 与 drop cache 并发触发死锁的问题
- 修复 LoongArch kvm 大页问题
- 修复 ARM64 mpam rmid 上限不正确的问题
- 修复 tty_jobctrl 潜在的 pid 内存泄露问题
- 修复 HISI_SAS 存在的硬盘 smart 信息概率获取不到问题
- 修复 X710 网卡，开机后报 “DCB init failed” 的问题
- 修复 net/mlx5 潜在的竞态导致内核崩溃的问题
- 修复 LTP/changemtu 测试 stmmac 失败的问题
- 修复 pcrypt 的 hang 住问题
- 修复 KVM 虚拟机 kvm run failed Bad address 报错的问题
- 修复 block 子系统 multi-vec 引入的内核崩溃问题
- 修复 NVMe Poll 队列为 0 导致某些情况下数据无法落盘的问题
- 修复 NFS 在某些错误故障情况下引起的崩溃问题
- 修复 XFS 在某些特定情况下，PageCache 未同步导致数据不一致的问题
- 修复 XFS 文件系统 xlog_grant_head_wait 在等待某些条件而进入 Hung 住的问题
- 修复 S5000c 中断自适应框架的 pci_irq_vector 警告问题
- 修复 eBPF 程序在某些情况下 bpf_overflow_handler 检查而导致内核崩溃的问题

- 修复 Blocktest 测试 NVMe 相关测试程序而导致内核崩溃的问题
- 修复 cgroup 在限制 Buffer IO 时，有可能无法限制住的问题
- 修复 ipset 在 destroy 和 test 之间的竞态问题
- [KYSEC] 修复 kysec_hash_sha256 某些错误情况下内存泄露的问题
- [KYSEC] 修复 kysec/exectl 运行启动时间过长的问题
- [KYSEC] 修复打开龙芯浏览器后开始菜单卡顿的问题
- [KYSEC] 修复 kysec 网络认证程序不断弹窗导致开机卡住的问题
- [KYSEC] 修复 kysec_notify_thread 在某些情况下会导致 Soft Lockup 的问题
- [KYSEC] 修复 kysec 在写入数据进 AUFS 时潜在的死锁问题
- [KYSEC] 修复 kysec/netctl 潜在的内存泄露问题
- 修复 HYGON 在 retbleed 漏洞无效的问题
- 修复 NFS 在某些情况下导致 Soft Lockup 的问题
- 修复 blktest block/001 测试失败的问题
- 修复 smartpqi 在 ARM64 服务器上，潜在的无法启动的问题
- 修复串口驱动 8250_port 的崩溃问题
- 修复 gauessdb 数据库 dorado 使用 ext4 文件系统时延高的问题
- 修复某些情况下 XFS 存在的启动数据不一致的问题
- 修复设置 cgroup cpu.rt_runtime_us 过大导致容器运行卡住的问题
- 修复 NGBE 驱动加载 xdp 驱动告警问题
- 修复 QLogic ISP2722 无法访问 VPD 的问题

- 修复 EXT4 文件系统在 Blocksize 为 64k 时，单目录超过 1200W 会文件系统奔溃的问题
- 修复某些 X86 设备的 /proc/cpuinfo 下获取的频率不准确的问题
- 修复 memcg 在极限情况下存在的内核 idr 竞态导致系统崩溃的问题
- 修复 blkmq 在某些情况下导致 kdump 无法正常生成的问题
- 修复 spi/spi-phytium 存在的空指针引用问题
- 修复 btrfs 文件系统在 fs_fill 测试项失败的问题
- 为捕获内核预留更多的内存，修复 Loongarch 下 kdump 失败的问题
- 修复 cgroupv2 在 frozen 时报告警告的问题
- 修复亲和调度导致 specjvm 性能下降的问题
- 修复 x86 架构在 fentry/fexit 失败的问题
- 修复 eBPF fentry/fexit 在 X86 架构加载失败的问题
- 修复 eBPF bpf_event_output 重入引起内核崩溃问题
- [KYSEC] 修复联网管控设置 httpd 服务联网策略为阻止后，依然可以联网的问题
- 修复 proc/fd RCU 引用计数警告问题
- 修复 cgroup/cgroup_attach_task_all 潜在的锁故障问题
- 扩充 ARM64 BPF JIT memory range 空间，让容器 POD 可以在单系统运行更多
- Loongarch 架构 spi-ls 驱动累计更新
- 修复 Intel EX710 网卡，系统自带驱动查看不到光模块信息的问题

- 修复 NTFS/fuse 格式的 U 盘挂载后重启，会卡在麒麟 LOGO 界面的问题
- 修复某些早期 Intel 设备在关闭 HPET 时钟源的情况下，TSC 不稳定而选择 jiffes 时钟的问题
- 修复飞腾 I2C 驱动在设备树模式下，内核崩溃的问题
- 修复某些网卡驱动未实现 gettime64 而导致运行 PTP 协议时，内核崩溃的问题
- 修复中断快速亲和切换导致某些外设中断被丢弃的问题
- 修复 ARM64 PG_dcache_clean 标志位设置存在的竞态问题
- 修复 bpf_map_update_elem 在极限情况下存在的内存泄露问题
- 修复调度进程无法唤醒导致 Livepatch 在申威架构失败的问题
- 修复在某些极限情况下，bpf_map_update_elem 之后内存泄露问题
- 修复在某些 efi 固件上，内核运行 efi-runtime 导致无法启动的问题
- 修复 ixgbe 驱动在 Intel 82599 网卡上使用 ethtool 无法让指示灯闪烁的问题
- 修复 CONFIG_ARM_SPE_PMU 驱动默认加载导致某些不支持该 PMU 的设备警告的问题
- 修复 txgbe SRIOV 启动/停止错误的问题
- [KYSEC] 修复 device_bind_driver 卡住的问题
- 修复飞腾 S5000c RAS 内存隔离与 CPU 隔离失败的问题
- 修复 swap 内存交换潜在的 RACE 竞态导致的空指针崩溃问题
- 修复 samba/cifs 在 ARM64 架构 64k pagesize 下读性能较差的问题

- 修复在某些早期板卡不支持 64bit MSI 中断时，其读写超时的问题
- 抑制 netdev_rx_csum_fault 在 csum 失败时的重复信息打印
- 修复 mlx5 网卡在极限内存申请失败的情况下，内核崩溃的问题
- 修复 NVMe 内核优化自适应程序在属性冲突时，设置失效的问题
- 修复 LTP/dio 测试失败的问题
- 暂时由于其闭源 .o 部分与内核代码冲突，关闭 sietium GenBu01 显示驱动
- 修复内核 kysec 进程防杀死中，获取的文件路径与实际文件路径不一致的问题
- 修复 LSM 堆栈化导致 selinux 状态错误无法启动 podman 容器的问题
- 修复 eBPF map 无法储存内部指针的问题
- 修复 K8S 1.24 kube-proxy ipvs 模式的 conn_reuse_mode 问题
- 修复由于新引入的 IPVLAN_MODE_L2E 导致与 Upstream 行为不一致的问题
- 修复 oomkiller 机制杀死 Nginx 子进程而非主进程导致的容器无法重启的问题
- 修复 eBPF 程序超过 1 个子程序时，运行失败的问题
- 修复 kmemleak_scan 在扫描内存时，可能引发越界访问的问题
- 优化内存遍历扫描机制，降低 S2500 在 FIO 测试 4k 大小 IO 时，设备卡死的问题
- LTP dio 项运行失败
- 修复 loongarch 平台 echo l > /proc/sysrq-trigger 的 bactrace 乱序的问题

- 修复长时间睡眠的任务唤醒后因为 vruntime 不正确出现调度饿死
- 修复在线离线混部在离线优先级负载均衡导致离线进程 D 状态挂死的问题

- 修复 Arm64 TRACING 类型的 eBPF 程序无法正确识别 btf 信息修正数据访问的问题
- 修复某些函数没有被 BTF 正确识别的问题
- 修复 Arm64 syscalls 无法被正确跟踪的问题
- 修正 Arm64 的 syscalls:sys_exit_execve 无法触发的问题
- 修复 xfs 文件系统潜在的 link_path_walk 指针为空的崩溃问题
- 修复 fill_kobj_path 在竟态时 slab-out-of-bounds 问题
- 修复 xhci_endpoint_reset 在状态发生变化时的竟态问题
- 修复 XHCI 驱动问题导致 BMC 远程开关机出现键鼠无功能现象
- 修复 MUCSE 沐创网卡 ethtool -t 命令失败的问题
- 修复 kysec 自 enable 到 disable 切换期间的潜在的内核崩溃问题
- 修复 kysec 默认情况下状态位异常导致系统重启失败的问题
- 修复 LTP oom01 测试项失败的问题
- 修复 LTP openat04 和 creat09 失败的问题
- 修复 Loongarch 架构的 LTP cpuhotplug04 失败问题
- 修复 KASAN: stack-out-of-bounds Read in unwind_next_frame 问题
- 修复 S2500 的自动调优程序潜在的崩溃问题
- 修复 Loongarch 架构概率 PCIe 无法唤醒的问题

- 修复 Loongarch 下 ltp bpf_prog02 测试失败的问题
- 修复 PCIe Hotplug 在虚拟机卸载再挂载过程中导致概率无法重新挂载的问题
- 优化 kysec 内存锁布局，提升鲲鹏 920 UnixBench 性能
- 修复 kysec devctl 潜在的死锁问题
- 修复开启 selinux 之后无法更改主机名称的问题
- 优化 kysec 在服务器内核上默认启用逻辑，优化 UnixBench 性能
- 修复 kysec-sync-daemon 引起的 CPU 使用率 100% 问题
- 修复 kysec 的越界访问问题
- 修复 PCIe 热插拔内存分配问题
- 修复 LTP inotify12 测试项失败的问题
- 修复 bpf_map_do_batch 存在的死锁问题
- 修复 cgroup 潜在的 percpu 内存未及时释放而存在的内存泄漏问题
- 修复 ICE 驱动引发的 XDP 警告问题
- 修复 SCHED_QOS 引发的内核崩溃问题
- 修复 blk-throtle 的 IO 在 dispatching 存在的竞态问题
- 修复 xfstest generic/232 出错的问题
- 修复混部特性 CPU burst 配置异常后，影响后续正常配置的问题
- 修复混部特性 unthrottle_cfs_rq wanring 的问题
- 修复某些特殊 NVMe 磁盘在软 RAID10 模式下存在 DISCARD 命令耗时较长的问题

- 修复 ARM64 平台 BPF JIT 的大小限制问题
- 修复申威架构编译出的内核包，没有 vmlinux 文件的问题
- [kysec] 修复 kysec 在移除目录时潜在的内核崩溃问题
- [kysec] 修复 kysec_free_sb 在某些情况下的 NULL 指针引用问题
- 修复 Loongarch 平台由于 PLT size 过大导致 LTP 大压力测试卡住的问题

- 修复 X86 架构上，Windows 虚拟机安装麒麟系统时，无法启动的问题
- 修复网讯网卡驱动 txbge 在 Power Systems 上驱动崩溃问题
- 修复百信服务器 LS7A2000 GNET 网络端口问题
- 修复 xfstest xfs/513 测试失败问题
- 修复 xfs 在强制关闭文件系统时，潜在的 Use-After-Free 的问题
- 修复 IO_URING 在注册时申请失败内存导致 double free 的问题
- 修复 l2cap_chan_del 报告的内核警告问题
- 修复 cfg80211_registered_device 的 key 检查警告问题
- 修复 memcontrol 的 thp_fault_alloc 和 thp_collapse_alloc 越界访问问题
- 修复 xfstest generic/586 问题
- 修复 xfstest xfs/641 问题
- 修复 xfstest xfs/643 问题
- 修复浪潮显示在 reboot 时，Legacy 模式可能存在黑屏的问题
- 修复 i2c designware 内存越界问题
- [kysec] 修复由于递归操作导致内核栈溢出而崩溃的问题

- 修复 Loongarch 架构内核启动报错的问题
- 修复 Sunway 架构 mremap04 失败的问题
- 修复 xfs 文件系统某些情况下，申请内存失败导致系统崩溃问题
- 修复 l2cap_sock_release 引起的 UAF 问题
- 修复 tun_free_netdev double free 的问题
- 修复 register_netdevice 潜在的内存泄露问题
- 修复华为 HNS 驱动 RDMA 导致系统卡住的问题
- 修复华为 iBMA 驱动空指针引用问题
- 修复 mac80211/sta_info 潜在的内存泄露问题
- 修复 net/tun 子系统潜在的 Use-After-Free 问题
- 修复 cfg80211 潜在的空指针崩溃问题
- 修复 nvmet_auth_set_key 潜在的内存泄露问题
- 修复 ieee802154/nl-mac 潜在的空指针崩溃问题
- 修复 Renesas uPD72020x 潜在的 FT2000+ 设备无法启动问题
- 修复 build_all_zonelists 与 page_alloc 之间的竟态问题
- 修复 mld_newpack 内存泄露问题
- 修复飞腾服务器同一个 I2C 通道同时访问 2 个 I2C 从设备会导致系统崩溃的问题
- 修复 LSI Megaraid 卡提示内存申请空间不够的问题
- 修复 Kpatch 工具生成热补丁后加载时出现符号未定义错误
- 修复 vfs_getxattr_alloc 潜在的内存泄露问题

- 修复 netfilter/ebtables 潜在的内存泄露问题
- 修复 netfilter/br_netfilter 潜在的内存泄露问题
- 修复 ipv6_renew_options 内存泄露问题
- 修复 __xfrm_policy_check 引用计数泄露问题
- 修复 tipc_sk_create 引用计数泄漏问题
- 修复 u32_init_knode 潜在的内存泄露问题
- 修复 ieee802154_raw_deliver 潜在的内存泄露问题
- 修复 cfg80211_bss_update 潜在的内存泄露问题
- 修复 rds_recvmsg 潜在的内存泄露问题
- 修复 qrtr_tun_open 潜在的内存泄露问题
- 修复 __ieee80211_beacon_get 潜在的内存泄露问题
- 修复 ieee80211_check_fast_xmit 潜在的内存泄露问题
- 修复 iscsi_cls_conn 与 sysfs 接口竞态问题
- 修复 4.19.90-27.rc3.v2101 内核后，nfs 客户端端口使用 1024 以下的问题
- [kysec] nfs 应用联网控制时，内核没有发同步消息给核外，无法弹框，导致 mount.nfs 服务失败的问题
- [kysec] overlay 环境下 loginid 不正确，导致三权分立模式下，用户权限不正常的问题
- 修复 Loongarch 在虚拟机进行 kdump 时，内核 stuck 的问题
- 修复海光虚拟机 NMI watchdog 功能异常，未按预期规律性上报 NMI 中断的问题

- 修复 IO_URING provide_buffers 申请过大导致内存消耗崩溃问题
- 修复 Hisi_SAS NCQ 场景盘出错期间，芯片连续 4 次拒掉新 IO 后，内核会关闭 NCQ 模式而影响 IO 性能的问题
- 修复 io_uring 在创建时失败的内存泄露问题
- 修复系统丢包，系统日志查看内核 neighbour table overflow 错误的问题
- 修复 Loongarch 核心崩溃信息存储到本地，无法成功重启的问题
- 修复 Loongarch 四路 3C5000 默认固态系统盘插槽安装系统失败的问题
- 修复兆芯 USB 鼠标在 S4 后失效问题
- 修复 enqueue_task_fair 内核打印警告信息的问题
- 修复 openvswitch/ovs 测试 cpu 飙升问题
- 修复 socket 在释放时，多余的 sock_owned_by_me 导致的警告问题
- 修复 bpf 子系统 update/delete ops 操作在某些内存申请故障下，内存泄露问题
- 修复蓝牙驱动在特殊情况下，不停打印错误信息的问题
- 修复 perf_event_open() 返回的文件描述符的第二次映射出错的问题
- 优化 ARM64 barrier 逻辑，修复潜在的崩溃问题
- 修复 NFS 读写时，内存故障导致系统崩溃问题
- 修复 clear_gigantic_page_chunk 错误的循环跳出条件使得某些内存页没有被清理而导致的问题
- 修复 kselftest/tls 错误
- 修复 Loongarch 架构上，Modules PLT 过大，导致大压力 LTP 测试时，加

载死机的问题

- 优化 CFS 在鲲鹏 920 上的内存释放判断逻辑，提升 UB 性能
- 修复部分 kselftest/bpf 自测问题
- 修复 Loongarch 下 PXE 挂在 NFS 时，网络超时的问题
- 修复 io_uring 的 iopoll.t 自测程序在 ext4/xfs/block_dev 下的失败问题
- 修复 io_uring 自测程序 accept-link 测试发现的崩溃问题
- 修复 mpt3sas 驱动在某些情况下，内核崩溃的问题
- 修复鲲鹏 920 架构下，某些特定的配置选项下，错误释放 early_memory 导致内核崩溃的问题
- 修复 io_uring 在执行 cancel request 时，存在的竞态问题
- 修复 xfs 文件系统在 xfstest 测试项下，quota 选项错误的问题
- 修复 xfs 文件系统在 xfstest 测试项下，xfs/510 测试子系统失败的问题
- 修复网络协议栈在某些特定的情况下，kfree_skb 会出现空指针引用的问题
- 修复 ALSA 音频子系统在读取 sys 接口时，出现 Use-After-Free 的问题
- 修复 Intel 架构虚拟机情况下，EDAC skx 错误的打印无法获取 tolm/tohm 的问题
- 修复 sched 某些情况下空指针异常
- 修复 xfstest/499 自测项问题
- 修复 cgroup_sk_alloc 不匹配的 percpu_ref_put 问题
- 修复 eBPF 自测问题
- 修复 stmmac is_jumbo 未初始化问题

- 修复 Loongarch 架构，由于 CMDLINE 长度限制导致 kdump 无法使用的问题

8. 附录 4 核外问题修复

8.1. abrt：

- 修复卸载 abrt-addon-ccpp 时的报错问题

8.2. accountsservice：

- 代码中一处宏定义，代码中作为数字使用，修改前版本中将其定义为字串类型，此次升级修复了此问题，使得用户可以通过 Accountsservice 服务获取正确的用户列表

8.3. aide：

- 修复“执行"aide --verbose=0"或"aide --verbose=1"命令后回显信息末尾未换行”问题。
- 修复“aide 命令行参数--report 指定为 https/http/ftp 格式的 URL 时出现 coredump”问题。
- 修复 aide 包执行”aide --check”命令，偶现 coredump 问题。

8.4. amanda：

- CVE-2023-30577

- CVE-2022-37704
- CVE-2022-37705
- 修复 hexencode 测试用例失败

8.5. anaconda：

- 修复系统存在/usr/bin/liveinst 空链接文件的问题
- 修复安装期间部分字符串未翻译的问题
- 修复 anaconda 使用 kickstart 文件方式，将系统安装到带有 WiFi 适配器的硬件以及没有电缆连接到任何 LAN 接口的硬件上时崩溃的问题
- 修复 UEFI 平台，ks 文件中 bootloader --leavebootorder 与 kernel cmline 中 inst.leavebootorder 无法正常工作的问题

8.6. anaconda-user-help：

- 修复 license 版本有歧义的问题

8.7. anthy：

- 修复地名描述错误

8.8. apache-commons-fileupload：

- CVE-2023-24998：由于 Apache Commons FileUpload 在处理用户的文件上传请求时未对文件数量进行限制，攻击者可通过上传大量文件造成拒

绝服务。

8.9. apache-commons-net：

- CVE-2021-37533,

8.10. apache-sshd：

- CVE-2022-45047，使用 Java 反序列化加载序列化 java.security.PrivateKey，攻击者利用该漏洞可以选择加载一个主机密钥 SSH 服务器

8.11. apr：

- CVE-2022-24963,

8.12. apr-util：

- CVE-2022-25147，apr_base64 函数中的整数溢出或回环漏洞允许攻击者超出缓冲区范围进行写入

8.13. argon2：

- 修复 readme 中的单词拼写错误

8.14. arm-trusted-firmware：

- CVE-2022-47630,

8.15. audit：

- 修复 krb5 的多处内存泄漏

8.16. augeas：

- 修复 augtool 命令执行出现 segfault 问题

8.17. authselect：

- popt 包存在内存泄漏问题，上游社区进行了修复，所以使用 popt 库的 authselect 包也添加 patch 进行相应的加固类修改

8.18. avahi：

- CVE-2023-1981，avahi 守护程序可能会被无特权用户发出的 dbus 调用时出现的本地崩溃，导致拒绝服务。
- CVE-2023-38470， avahi_escape_label() 函数中存在可达断言。
- CVE-2023-38469， avahi_dns_packet_append_record 中存在可达断言。
- CVE-2023-38471，，dbus_set_host_name 函数中存在可达断言。
- CVE-2023-38472， avahi_rdata_parse() 函数中存在可达断言。
- CVE-2023-38473， avahi_alternative_host_name() 函数中存在可达断言。

8.19. bacula：

- 解决停止 bacula 服务时进程没有正常退出的问题

8.20. bamf：

- 修复了 current_desktops 变量未释放导致的内存泄漏问题
- 修复 bamf 服务卸载时的警告信息

8.21. bash：

- 修复子进程的条件竞争问题。
- 修复对多实例的解析逻辑问题。
- 修复了 nowork comsub 命令打印问题；
- 修复 globbing 中少量的内存泄漏。
- 修复了使用匹配多个文件的 glob 模式完成命令字时的泄漏问题；当局部变量被重置时，在取消设置时保留导出属性；已修复在执行字符集转换时使用 nllanginfo 的问题

8.22. batik：

- CVE-2022-41704 涉及通过特定类型的脚本（如 Java 脚本）在 Batik 处理 SVG 文件时执行未授权的代码。
- CVE-2022-42890 涉及在处理 SVG 文件时，通过 Rhino JavaScript

引擎暴露过多的 Java 类给脚本的问题。

8.23. bcc：

- 修复./tcpconnect 的时候会出现 bpf 编译报错的问题

8.24. bind：

- CVE-2023-3341
- CVE-2023-2828
- CVE-2022-2906，
- CVE-2022-2881
- CVE-2022-2795
- CVE-2022-38178
- CVE-2022-38177
- 修复安装 bing-sdborbing-sdb-chroot 的错误输出
- 修复重定向问题，
- 修复 new_zone_lock 加锁问题等

8.25. binutils：

- 修复 gold 链接器开启"-q"选项时生成的重定位信息错误
- 修复 gold 链接签名移位逻辑错误
- CVE-2022-47008，在返回值为 NULL 时，free(tmpname)，释放 tmpname

- CVE-2022-47011，路径失败时没有释放 fields 变量
- CVE-2022-47696， objdump 缺陷引起的服务拒绝类安全漏洞
- CVE-2022-48064，通过 dwarf2.c 中 bfd_dwarf2_find_nearest_line_with_alt 内存过量消耗漏洞。攻击者使用伪造的的 ELF 文件用于 DNS 攻击。
- 修复 binutils-help 降级后卸载有部分文件找不到问题
- 修复未定义的移位和整数溢出问题
- 修复 nested_arch->file 的 use-after-free 问题
- CVE-2021-46174， objdump 模块 bfd_getl32 函数中的堆缓存移除漏洞

8.26. bison：

- CVE-2020-24240

8.27. bluez：

- CVE-2021-0129
- CVE-2022-0204
- CVE-2021-41229
- CVE-2022-39176
- CVE-2022-39177
- CVE-2023-27349

8.28. bouncycastle：

- CVE-2023-33201，如果生成一个自签名证书，其主题名称包含特殊字符，会使攻击者能够在搜索查询中指定其他属性,从而导致信息泄漏。

8.29. bval：

- 解决 xstream 升级导致的编译问题

8.30. byacc：

- CVE-2021-33641，处理注释时，malloc 函数错误地访问了已释放的内存（使用后释放）。
- CVE-2021-33642，当处理文件时,在 more_curly()函数的 next_inline()中发生了无限循环

8.31. caja：

- 修复更改 dvd 容量显示错误问题
- 修复内存泄漏

8.32. c-ares：

- CVE-2022-4904：ares_set_sortlist 函数调用 config_sortlist 函数来解析输入字符串并初始化 sortlist 配置。ares_set_sortlist 没有对输入字符串

的有效性进行任何检查，有可能在 config_sortlist 函数在调用 memcpy 函数时，产生堆栈溢出，导致缓冲区溢出攻击。

- CVE-2023-32067：当目标解析器发送查询，攻击者伪造一个长度为 0 的畸形 UDP 报文返回给目标解析器。目标解析器错误地将 0 长度理解为连接的正常关闭，解析失败，实现 DoS 攻击，拒绝服务。
- CVE-2023-31130：ares_inet_net_pton() 容易受到某些 ipv6 地址的缓冲区下溢的影响，特别是 0::00:00:00/2。在 ares_inet_net_pton()中存在缓冲区溢出，导致拒绝服务。
- CVE-2023-31124：当交叉编译 c-ares 并使用 autotools 构建系统时，不会设置 CARES_RANDOM_FILE,就像交叉编译 aarch64 android 时一样。这将降级为使用 rand（） 作为回退，这可能允许攻击者通过不使用 CSPRNG 来利用熵的不足。
- CVE-2023-31147：当/dev/urandom 或 RtlGenRandom()不可用时，c-ares 使用不安全的 rand()生成用于 DNS 查询 ID 的随机数，rand()函数的输出容易受到攻击者的预测和破解，对于这种可预测的输出，可能会导致数据泄漏。

8.33. catfish：

- 修复了排除路径不生效，符号链接丢失的问题

8.34. ccid：

- 修复 eToken-5110 设备支持的问题

8.35. cdrkit：

- 修复在 gcc 10 上编译失败的问题
- 修复系统中存在空链接文件的问题

8.36. ceph：

- CVE-2020-12059，带有无效标签 XML 的 POST 请求会触发空指针异常，从而导致 RGW 进程崩溃
- 修复 2.4.3ceph-mgr 服务缺少 python2 安装依赖导致运行报错问题
- CVE-2020-25678， ceph 以明文存储 mgr 模块密码。可以通过搜索 mgr 日志时查看到明文密码
- CVE-2020-27781， 消费者可能会操纵和窃取用户凭证，导致潜在的特权升级
- CVE-2020-10753， Ceph 存储 RadosGW,当发出 CORS 请求时，CORS 配置文件中 ExposeHeader 标记中的换行符在响应中生成一个头注入
- CVE-2021-3524,CVE-2020-10753 之前的 bug 修复没有考虑使用 r 作为标题分隔符，因此产生了一个新的缺陷
- CVE-2020-1760，支持 Amazon S3 中匿名用户发送的请求
- 解决 mempool.h 函数 pick_a_shard 明显的性能问题
- 解决 ceph dh 功能不可用问题

- CVE-2021-3979，使用 ceph-volume 创建的加密设备的密钥长度不正确
- 解决 rgw 启动失败问题
- CVE-2023-43040，在 rgw 中发现了一个缺陷。如果 aPOST 的表单数据中包含一个名为 bucket 的键，其值与用于签名请求的桶的名称匹配，则该缺陷允许非特权用户向给定键可访问的任何桶写入数据

8.37. cifs-utils：

- 将缺少的位置处理添加到装载参数 gid/backup_gid/snapshot，解决每次通过复制和粘贴将新参数添加到末尾时，字符串位置都不会更新。
- 修复概率编译错误。
- 修复解析快照时的最大缓冲区大小。
- 修复装载点不存在时的崩溃问题。
- 修复 kerberos 装载中的问题。
- CVE-2022-27239，解析 mount.cifs ip=命令行参数时，基于堆栈的缓冲区溢出可能导致本地攻击者获得 root 权限。
- CVE-2022-29869，字符但不是有效的凭据文件时，cifs-utils 到 6.14 以及详细的日志记录可能会导致信息泄漏。

8.38. clamav：

- 修复 clamav-clamonacc.service 服务启动失败
- 修复执行 clambc 命令失败

- 修复 clamonacc -w 命令执行报错
- CVE-2023-20032，HFS+分区文件解析器中的漏洞可能允许未经身份验证的远程攻击者执行任意代码。此漏洞是由于缺少缓冲区大小检查而导致的，该检查可能导致堆缓冲区溢出写入。
- CVE-2023-20052： 文件解析器中的漏洞可能允许未经身份验证的、远程攻击者访问受影响设备上的敏感信息。此漏洞是由于启用可能导致 XML 外部实体注入的 XML 实体替换。攻击者可以通过提交精心制作的 DMG 文件以供受影响设备上的 ClamAV 扫描来利用此漏洞。成功的利用可能允许攻击者从 ClamAV 扫描进程可能读取的任何文件中泄漏字节。
- CVE-2023-20197：ClamAV 的 Hierarchical File System Plus（HFS+）文件系统映像解析器中存在一个漏洞，允许未经身份验证的远程攻击者在受影响的设备上造成拒绝服务（DoS） 情况。

8.39. clevis：

- 修复了使用 TPM2 PIN 解析 PCR ID 的问题
- 解决 systemd 中 /dev/fd/X 的删除问题
- 修复带有空格的密码错误
- 修复 clevis-luks-regen 中使用 return 而不是 exit 的问题
- 修复 clevis luks bind 中 -t 选项的问题
- 修复 clevis-encrypt-tang 在指定 SHA-256 thumbprint 时的问题

8.40. cloud-init：

- 解决安装 cloud-init 重启系统后语言环境配置改变的问题；
- CVE-2022-2084，敏感数据可能会暴露在版本 22.3 之前的可读日志中。
- CVE-2023-1786，用户数据文件权限优化；

8.41. cloud-utils：

- 修复重启系统后语言环境由之前配置变为英文问题

8.42. cockpit-appstream：

- 修改虚机创建相关 JS 模板，修复无法创建虚拟机的 bug.

8.43. cockpit：

- CVE-2021-3660,

8.44. console-setup：

- 修复地名错误

8.45. containerd：

- 增加 cgo 安全编译选项,使用 pie 构建模式，增强程序安全性，使其无法被反编译。
- CVE-2022-23471，解决 exec 中协程泄露问题。

- 修复 k8s 场景下由于未导入上下文导致构建失败的问题
- CVE-2023-25153 CVE-2023-25173，在导入 OCI 映像时，对某些文件的读取字节数没有限制，如果恶意制作的映像文件较大且未应用限制，则可能导致拒绝服务
- 修复 systemd-journald 异常情况下会导致 shim 写日志卡住从而导致 exec/inspect 卡住的问题
- 修复可靠性测试中 containerd 相关目录资源残留问题
- 修复 walkingDiff 方法中临时 mount 错误处理问题
- 修复无效验证错误检查问题
- 修复 For 循环中的隐式内存别名问题
- 修复增加 cio.Cancel()关闭管道逻辑问题
- 修复无法多次 checkpoint 容器的问题
- 修复为 cgroup v1 内存使用添加 nil 指针检查问题
- 修复允许连接到 stdin/stdout/stderr 的任意组合问题
- 更新 bump ttrpc 版本，增加 ErrUnexpectedEOF 错误过滤

8.46. coreutil：

- 修复 xstrtol()函数的错误使用，xstrtol()函数不会设置可靠的错误码。
- 解决 glibc strtold ("NaN", ...)函数返回的 long double 包含未初始化的位的问题
- 修复 df 模块的内存泄漏的问题

- 修复 ls -l 命令会触发 autofs mounts 的策略问题
- 修复 stat --cached=never 命令会触发 autofs mounts 的策略
- 修复 printf 对"\r\n"的打印错误
- 修复 print_page()一直返回 True 导致的 pr 命令错误
- 修复 truncate 非法 seek 操作

8.47. cpio：

- CVE-2015-1197
- CVE-2021-38185

8.48. cracklib：

- 修复没有输入数据的情况下，截断字典文件的问题。
- 修复简单密码的长度错误，30->32

8.49. crash：

- 修复打开 CONFIG_KASAN=y 的编译选项，编译出的 kernel 上产生的 vmcore 文件，执行 bt 命令会有堆栈的截断的问题
- 修复在使用 dis 进行包含点积指令(sdot)的堆栈解析的时候，能够发现 sdot 指令不能正常显示的问题

8.50. cronie：

- 修复某些杀毒软件禁止用 fclose 关闭标准输入，导致 cronie 每日定时任务调用失败的问题

8.51. crypto-policies：

- 解决编译问题:nss 组件在 3.59 版本开始新增了部分算法（ECDSA RSA-PSS RSA-PKCS），nss 升级到 3.59 及之后版本后，由于 crypto-policies 提供的安全配置中不支持 nss 新增算法，导致编译失败；
- 解决编译依赖，asciidoc 升级为 10 后，不再提供 asciidoc.py 脚本提供的命令；

8.52. cryptsetup：

- 修复 CVE-2020-14382 ，32 位系统下的内存越界问题。
- 修复问题：修复哈希算法的名称中有中横线引发的 integritysetup 中的问题。
- 修复问题：修复用于处理 ECB 模式的后端加密的问题。
- 修复问题：修复某些 BitLocker 设备的未指定扇区大小的错误，在未指定扇区大小的情况下应该使用 512 字节的扇区大小。
- 修复问题：修复读取 BitLocker 兼容模式下的元数据中的 key 的大小的问题。
- 文档修改：修复文档中的拼写错误。
- 修复问题：修复从交互式终端部分读取密码短语的问题。

- 修复问题：修复通过终端输入的密码的最大长度。现在，交互式密码短语的最大长度正好是 512 个字符（不是 511 个）。
- 修复问题：veritysetup 修复 verityFEC。
- 优化：veritysetup 即使 root 哈希失败，也要运行 FEC 修复检查。
- 修复问题：修复 BitLocker 扫描过程中设备消失时发生的故障。
- 修复问题：修复 LUKS1 修复代码（自 1.7.x 版本以来的回归）。
- 修复问题：修复 LUKS2 的 luksKeyChange 和已分配的令牌。
- 修复问题：修复使用 LUKS2 令牌调整 cryptsetup 大小的问题。
- 修复问题：修复重新加密中的默认 XTS 模式密钥大小。
- 修复问题：修复许多关于使用 cipher_null（空调试密码）的问题。修复包括：
- -修复 LUKS2 中检测到空密码的错误。cipher_null 不再可能用于密钥批量加密，在 LUKS2 中，它只能用于调试目的的数据。
- 修复问题：修复了 libpassphdqc 2.0.x（可选密码短语质量检查）。
- 修复问题：修复了各种代码分析工具发现的问题。
- 修复问题：修复包括对 libpopt 命令行选项字符串泄漏的返工。
- 修复问题：手册页的各种修复。
- 修复问题：integritysetup：修复可能的 dm 完整性映射表截断。
- 修复问题：针对常见警告生成的其他修复程序和解决方法通过一些静态分析工具（如 gcc-11 分析仪）和其他代码强化。
- 修复问题：修复编译测试的独立 libintl 检测。

- 修复问题：修复了 OpenSSL3 默认的 OpenSSL crypt 后端支持。对于 OpenSSL 版本 3，我们需要加载旧哈希的遗留提供程序和密码。
- 修复问题：修复使用 LUKS2 令牌调整 cryptsetup 大小的问题。
- 修复问题：修复了在没有 dlvsym（）的情况下编译 libc 实现的问题。一些替代的 libc 实现（如 musl）没有提供版本符号 dlvsym 函数。代码现在回退到 dlsym 用于动态 LUKS2 令牌加载的操作。由维护人员来确保 LUKS2 令牌插件已为支持的版本编译。
- 修复问题：修复具有非标准库的系统上的编译和测试（独立的 argp 库、外部 gettext 库、BusyBox 标准工具的实现）。
- 优化：尝试在没有 udev 支持的系统上解决一些问题。注意：非 udev 系统不能为内核提供所有功能设备映射器，并且某些操作可能会失败。
- 修复问题：修复了 OpenSSL3 加密后端（包括 FIPS 模式）。
- 修复问题：修复了 LUKS2 加密代码中的 offset 错误（如果使用了--offset 选项）。
- 修复问题：修复 LUKS1 cryptsetup 修复命令中的一些特定问题。

8.53. ctags：

- CVE-2022-4515，在 Exuberant Ctags 中发现了处理“-o”选项的方式存在缺陷，

8.54. cups-filters：

- CVE-2023-24805

8.55. cups：

- CVE-2022-26691，一个 cups 代码逻辑问题，应用程序可能能够获得提升的权限．在相关接口 ctcompare（ ）中增加输入值的空值判断从而解决此问题；
- CVE-2019-8842， 在某些配置中，远程攻击者可能能够提交任意打印作业；合入 OE 修改，在 ippReadIO 接口中修改相关配置，修复此问题；
- CVE-2023-32324，函数 format_log_line 中的缓冲区溢出漏洞可能允许远程攻击者在受影响的系统上造成 DoS。当配置文件 cupsd.conf 将 loglevel 的值设置为 DEBUG 时，可以触发漏洞利用。在_cups_strlcpy 增加 size 是否为 0 判断，修复此问题；
- CVE-2023-34241，CUPS 将空闲内存的数据记录到日志服务中时，会在连接关闭后记录，但应该是在连接关闭之前记录。
- CVE-2023-4504，由于验证攻击者特制的 PostScript 文档提供的长度失败，CUPS 和 libppd 容易受到基于堆的缓冲区溢出的影响，并且可能会执行代码。在 scan_ps 接口中增加如果达到 NULL 终止符则返回 NULL 修改，修复此问题；

8.56. curl：

- CVE-2023-32001

- CVE-2023-38545
- CVE-2023-38546
- CVE-2023-28320
- CVE-2023-28321
- CVE-2023-28322
- CVE-2023-27536
- CVE-2023-27535
- CVE-2023-27533
- CVE-2023-27534
- CVE-2023-27535
- CVE-2023-27536
- CVE-2023-27538
- CVE-2023-23916
- CVE-2022-32221
- CVE-2022-35252
- 解决启用--disable-http-auth 配置项时的编译失败问题

8.57. cyrus-sasl：

- 修复 cyrus-sasl 切换数据为 gdbm 后导致的认证报错问题。
- CVE-2022-24407，SQL 插件存在 SQL 注入攻击。由于未能正确转义 SQL 命令输入，远程攻击者可以利用此问题执行任意 SQL 命令

8.58. dbus：

- 修复 CVE-2022-42010,CVE-2022-42011,CVE-2022-42012

- 修复 CVE-2023-34969
- 修复策略创建失败可能导致崩溃的问题
- 解决某个客户端策略加载失败后可能导致崩溃的问题

8.59. deltarpm：

- CVE-2005-1849
- CVE-2016-9840
- CVE-2016-9841
- CVE-2016-9843
- CVE-2018-25032
- CVE-2022-37434

8.60. dhcp：

- CVE-2021-25214,包含 onwer name 而不是传输区域顶点的 SOA 记录的增量区域传输可能会导致接收报文的 named 服务器无意中删除对应区域的 SOA 记录；这将导致在对该区域进行下一次 SOA 刷新查询时断言失败；named 服务异常终止
- CVE-2021-25215,named 处理 DNAME 记录可能会触发多次增加 RRset 到 ANSWER 段，这可能会导致 bind 断言失败，named 服务将会异常终止
- CVE-2021-25219,攻击者可以利用 DNS lame cache 设计本身的缺陷，造成 DNS resolver 严重的性能下降，甚至可能造成拒绝服务攻击

- CVE-2021-25220，bind9 做为转发器时，假的 NS 记录也许会被转发器缓存，造成 DNS 转发器转发不正确的 answers。
- CVE-2022-2928 ，引用计数器可能会溢出并导致服务器中止
- CVE-2022-2929，一个可以访问 DHCP 服务器的系统，发送经过精心设计的包含超过 63 个字节的 fqdn 标签的 DHCP 数据包，最终可能导致服务器内存不足

8.61. djvulibre：

- CVE-2021-46310
- CVE-2021-46312

8.62. dmidecode：

- 修复字符串的 ASCII 过滤；
- 解决 dmidecode 命令-u 选项可能会导致崩溃问题。
- CVE-2023-30630

8.63. dnf：

- 解决下载失败时，错误提示可能为空的问题。
- 解决缺少历史 db 库时，dnf mark install 命令错误。
- 解决 dnf swap 命令无法加载本地包问题。
- 解决 group 被禁用时无法删除问题。

- 解决 dnf 扫描空目录时，触发崩溃问题。
- 解决 url 包含相对路径时，包下载失败问题。
- 解决/etc/dnf/vars 存在临时文件时，导致 dnf 崩溃问题。
- 解决 I/O busy 时，ctrl+c 终止 dnf install 报 AttributeError 问题。

8.64. dnsmasq：

- CVE-2020-25681
- CVE-2020-25682
- CVE-2020-25683
- CVE-2020-25684
- CVE-2020-25685
- CVE-2020-25686
- CVE-2020-25687
- 修复 DNS 回复通过错误的套接字发送问题。
- 修复 2.83/2.84 版本中 DNS 重试的问题。
- 调整 TFTP 代码以检查所有接收到的数据包的发送方。
- 支持输入标签与--tag-if 的一些通配符匹配。

CVE-2021-3448

- 修复导致 dnsmasq 在重负载下无法跟踪处理 TCP DNS 连接的进程的错误

8.65. docbook5-style-xsl：

- 修复安装后处理脚本报错

8.66. docker-engine：

- CVE-2023-25173，容器内未正确设置附加组。如果攻击者直接访问容器并操纵其附加组访问权限，他们可能能够使用附加组访问权限绕过某些情况下的主组限制，潜在地获取对敏感信息的访问权限或获取在该容器中执行代码的能力
- CVE-2023-25153，导入 OCI 镜像时，对于某些文件，没有对读取的字节数设置限制。如果使用恶意构造的包含未应用限制的大文件的镜像，可能导致 containerd 拒绝服务
- 解决 cgroup 嵌套和 kubepods 分层问题
- 解决 docker attach <容器 id>命令执行失败问题
- CVE-2023-28840，
- CVE-2022-24769，主要解决容器错误地以非空的可继承 Linux 进程能力启动导致进程安全泄露
- 解决执行 exit 退出终端后当前终端卡死问题
- 解决 dockerps 查询容器状态与实际 shim 进程状态不统一问题
- CVE-2022-36109，主要解决未正确设置 supplementary groups 问题
- 解决镜像 layer 回滚时可能遇到的镜像不完整无法修复问题
- 修复 dockerd core 数组越界问题

- 修复两次重新启动 dockerd 后丢失容器问题。
- CVE-2023-28840
- CVE-2023-28841
- CVE-2023-28842
- 修复在 docker pull 时重启 docker daemon 导致 thinpool 已满问题。
- 修复 blockThreshold 已满错误。

8.67. docker-proxy：

- CVE-28840，docker 的 swarm mode 在 xt_u32 内核模块不启用后加密策略失败问题

8.68. docker-runc：

- CVE-2022-29162,进程在 execve 期间权限提升，导致触发安全漏洞。
- 解决在使用 runc update 更新胖容器内存值时失败并回显设置 device.allow 被拒绝的问题

8.69. dosfstools：

- 修复 mkfs.fat 计算在非 512 字节的磁盘上的问题

8.70. dovecot：

- 解决关于 ABRT 错误的模糊测试问题；
- CVE-2020-28200

- CVE-2021-33515
- CVE-2022-30550；
- 添加安装依赖 tar，解决执行 dovecot-sysreport 命令报错

8.71. doxygen：

- CVE-2020-11022
- CVE-2020-11023
- CVE-2020-23064
- 修复 HTML 重新生成时的 label 名称错误问题

8.72. dpdk：

- 修复了对于 mlnx 驱动网络堆栈错误返回处理逻辑，CVE-2021-3839 CVE-2022-0669
- 修复了对于 vhost 标头触发构建拒绝服务的问题,CVE-2022-2132 CVE-2022-28199

8.73. dracut：

- 修复当/etc/ld.so.preload 文件中指定的库不存在时，一些符号链接不能被打包进 initrd 中的问题

8.74. e2fsprogs：

- misc/fsck.c: 修复 fsck -N 操作可能杀死其他进程的问题。

- debugfs：修复 logdump -O -n <num_trans>命令中的重复输出问题。
- libext2fs: 添加对 extent 操作的健全性检查，修复 CVE-2022-1304。
- e2fsck: 修复 ext2fs_extent_get 中 handle->level 溢出的问题。

8.75. ebtables：

- 修复 ebtables string 的 match 无法配置 string-icase 的问题；
- 修复安装时的报错 ；
- 修复降级异常打印“没有这样的文件或目录”；

8.76. ecryptfs-utils：

- 修复主机名映射配置默认不可用问题

8.77. edk2：

- CVE-2019-14584 EDK2 中的空指针取消引用可以允许经过身份验证的用户通过本地访问潜在地启用权限升级。
- CVE-2019-11098 EDKII 中 MdeModulePkg 中的输入验证不足可能会使未经身份验证的用户有可能通过物理访问升级权限、拒绝服务和/或信息披露。
- CVE-2021-38578 计算 BufferSize 时，SmmEntryPoint 中现有的 CommBuffer 检查将不会捕获下溢。
- CVE-2022-4450 JimuReport 中发现了一个漏洞。该操作导致注射。可以

远程发起攻击。

- CVE-2023-0401 当在 PKCS7 签名或signedAndEnveloped数据上验证签名时，可以取消引用 NULL 指针。缺少对初始化函数返回值的检查，这会导致摘要 API 的无效使用，很可能导致崩溃。
- CVE-2023-0215 API 函数 BIO_new_NDEF 是一个辅助函数，用于通过 BIO 流式传输 ASN.1 数据。在某些条件下,会发生释放后使用，这很可能会导致崩溃。
- CVE-2023-0286 存在与 X.509 GeneralName 内的 X.400 地址处理相关的类型混淆漏洞。
- CVE-2022-4304 OpenSSL RSA 解密实现中存在基于定时的侧通道，足以在 Bleichenbacher 式攻击中通过网络恢复明文。

8.78. efibootmgr：

- 修复了当传递的--index 大于当前启动顺序大小时出现的段错误

8.79. efivar：

- 修复 eMMC-s 的/sys/block-sysfs 解析；
- 修复 s{yt,ty}leefi_get_variable 中的打字错误(3)；
- 修复 nvme 子系统设备的解析；
- 尝试修复已识别的线程安全漏洞；
- 修复从 UTF8 到 UCS2 的转换；

- 修复 linux 虚拟根设备解析；
- efivar.spec.in：将许可证修复为有效的 SPDX；
- 修复编译时 mount.h 冲突问题。

8.80. elfutils：

- 修复卸载 elfutils-debuginfod-client-devel 时报错找不到/usr/lib64/libdebuginfod.so.1 文件的问题。
- 修复 eu-ar -r 命令将文件归档时权限发生变化的 Bug。
- 修复 eu-ar -ar 和 eu-ar -br 向归档文件内添加文件，导致文件丢失的 Bug。
- 修复 eu-ar -N 指定文件索引实际指定到了 N+1 的 Bug。
- 修复/usr/lib/systemd/systemd-sysctl 命令应用内核参数时，找不到 kernel/yama/ptrace_scope 文件的问题
- CVE-2021-33294，readelf.c 文件中的函数 handle_symtab 中发现了一个无限循环。这使得攻击者可以通过精心设计的文件造成拒绝服务
- 修复 eu-ar -m 的段错误 Bug。
- 完善 LoongArch 架构支持，解决 check 用例失败问题。

8.81. emacs：

- CVE-2022-45939
- CVE-2022-48337

- CVE-2022-48338
- CVE-2022-48339
- CVE-2023-28617

8.82. eom：

- 修复图像查看器查看历史图片软件闪退问题。

8.83. ethtool：

- 修复 ethtool 添加 vxlan 无响应的问题
- 修复 ethtool 不支持添加 vxlan 的问题
- 修复不支持设置和获取 rx buf len 和 rx push 的问题
- 修复内存泄露问题

8.84. evolution-data-server：

- CVE-2020-14928，存在影响 SMTP 和 POP3 的 STARTTLS 缓冲问题。当服务器发送“开始 TLS”响应时，eds 读取其他数据并在 TLS 上下文中对其进行评估，也称为“响应注入”

8.85. exempi：

- CVE-2020-18651
- CVE-2020-18652
- CVE-2021-36048

- CVE-2021-39847
- CVE-2021-42530
- CVE-2021-36046
- CVE-2021-36055
- CVE-2021-40716
- CVE-2018-12648
- CVE-2021-36054
- CVE-2021-36047
- CVE-2021-36052
- CVE-2021-36058
- CVE-2021-36045
- CVE-2021-42531
- CVE-2021-36064
- CVE-2021-42529
- CVE-2021-42528
- CVE-2021-36050
- CVE-2021-40732
- CVE-2021-36056
- CVE-2021-42532
- CVE-2021-36053
- CVE-2021-36051

8.86. exiv2：

- CVE-2019-13108，整数溢出允许攻击者通过精心制作的 PNG 图像文件导致拒绝服务（SIGSEGV），因为 PngImage::readMetadata 错误处理了 iccOffset 的零值。

- CVE-2019-13504，Exiv2::MrwImage::readMetadata 中存在越界读取。
- CVE-2021-31292，CrwMap::encode0x1810 中的整数溢出允许攻击者通过精心设计的元数据触发基于堆的缓冲区溢出并导致拒绝服务(DOS)。
- CVE-2021-32815， 修改精心制作的图像文件的元数据时，会触发断言失败。如果攻击者可以诱使受害者在精心制作的图像文件上运行 Exiv2，他们就有可能利用该漏洞导致拒绝服务。
- CVE-2021-37620， 读取精心制作的图像文件的元数据时，会触发越界读取。如果攻击者可以诱使受害者在精心制作的图像文件上运行 Exiv2，他们就有可能利用该漏洞导致拒绝服务。
- CVE-2021-37619， 元数据写入精心制作的图像文件时，会触发越界读取。如果攻击者可以诱使受害者在精心制作的图像文件上运行 Exiv2,他们就有可能利用该漏洞通过使 Exiv2 崩溃来导致拒绝服务。
- CVE-2021-34335，由于整数除以零导致的浮点异常
- CVE-2021-37618， 用于打印精心制作的图像文件的元数据时，会触发越界读取。如果攻击者可以诱使受害者在精心制作的图像文件上运行 Exiv2，他们就有可能利用该漏洞导致拒绝服务。
- CVE-2021-37621， 一个无限循环。当 Exiv2 用于打印精心制作的图像文件的元数据时，会触发无限循环。
- CVE-2021-34334， 用于读取精心制作的图像文件的元数据时，会触发无限循环。如果攻击者可以诱使受害者在精心制作的图像文件上运行 Exiv2，

他们就有可能利用该漏洞导致拒绝服务。该错误已在 v0.27.5 版本中修复。

- CVE-2021-37622,
- CVE-2021-37623,
- CVE-2021-37615，用于打印精心制作的图像文件的元数据时，会触发空指针取消引用。
- CVE-2021-37616，用于打印精心制作的图像文件的元数据时，会触发空指针取消引用。
- CVE-2022-3755,QuickTime 视频处理程序的文件 quicktimevideo::userDataDecoder .cpp 函数。该操作会导致空指针取消引用。攻击可能是远程发起的。
- CVE-2022-3756,视频处理程序的文件 quicktimevideo::userDataDecoder .cpp 函数。该操作会导致空指针取消引用。攻击可能是远程发起的。

8.87. expat：

- CVE-2022-25235：2.4.5 之前的 Expat 中的 xmltok_impl.c 缺少某些编码验证，例如检查 UTF-8 字符在特定 context.c 中是否有效。向 XML 处理应用程序传递格式不正确的 2 字节和 3 字节 UTF-8 序列时，容易触发漏洞。
- CVE-2022-25236：2.4.5 之前 Expat 中的 xmlparse.c 允许攻击者将名称空间分隔符插入到名称空间 uri 中。在“xmlns[:prefix]”属性值中传递一个或多个名称空间分隔符字符，会导致 expat 将格式不正确的标记名称发送给 XML 处理器，导致触发漏洞。

- CVE-2022-25313：在 2.4.5 之前的 Expat 中，通过 DTD 元素中较大的嵌套深度来触发 build_model 中的堆栈耗尽。解析一个 2 兆字节的文件且带有大量的开括号的文件时，触发 doctype 函数中的堆栈耗尽。
- CVE-2022-25314：在 2.4.5 之前的 Expat 中，copyString 函数中变量 charsRequired 类型为 int 型，存在整数溢出的缺陷。传入太大的参数，比如在 64 位机器上传入的值是千兆字节,影响解析器创建时的编码名称参数。
- CVE-2022-25315：在 2.4.5 之前的 Expat 中，storeRawNames 函数中存在整数溢出的缺陷。滥用 m_buffer 扩展逻辑，导致标签名的大小无限接近 INT_MAX 时，例如达到千兆字，再解析此标签名时，容易触发漏洞。
- CVE-2022-40674：在 xmlparse.c 的 doContent 函数中存在释放后使用的问题。
- CVE-2022-43680：libexpat-2.4.9 版本及以前，在内存不足的情况下，过度的销毁 XML_ExternalEntityParserCreate 中的共享 DTD 会导致内存 use-after-free。libexpat 组件包含 expat 组件的源码，expat 侧也需要修复。

8.88. fakechroot：

- 修复栈溢出、程序崩溃问题

8.89. fcitx-configtool：

- 修复输入法配置界面中的快捷键配置弹窗点击关闭按钮无反应

8.90. festival：

- 修复中文表述错误

8.91. ffmpeg：

- CVE-2021-38114
- CVE-2020-35964

8.92. file：

- CVE- 2022-48554

8.93. firefox：

- CVE-2020-15969，适配 linux 下使用于 sctplab 的 sctp 网络的浏览器问题，当 sctp 和 sctplab 网络使用 fuzzer_connect 函数后，存在超时等待的问题。
- CVE-2020-15999，当浏览器使用了 fontface 字体，Freetype 中的堆缓冲区溢出允许远程攻击者通过某些 HTML 页面，Load_SBit_Png 使用 freetype 的 Noto ColorEmoji 字体，在 gfx.downloadable_fonts.keep_color_bitmaps 存在某个漏洞。可以通过这个漏洞窃取到用户的信息，如信用卡。

- CVE-2020-16012，drawImage 时序取决于 alpha 通道值，允许读取跨域图像，glx 驱动当 CanvasRenderingContext2D::drawImage 调用 DrawTargetCairo::DrawSurface、PaintWithAlpha 、cairo_paint 、_cairo_gstate_paint 、_cairo_surface_paint 、_cairo_pattern_is_clear 、_cairo_surface_paint 等函数，在循环中调用 drawImage 也会导致整个系统变慢
- CVE-2020-26951-2 ，Firefox Nightly 进行模糊测试时，一个使用有效负载 <svg><style><title>[xssplyload] 绕过 HTML sanitizer，在其中嵌入代码，可以导致代码运行。
- CVE-2020-26953， DOMFullscreenParent.didDestroy() r=Gijs 调用 FullScreen.cleanupDomFullscreen()时处理 TypeError 和 InvalidStateError 出现错误日志，引起浏览器崩溃
- CVE-2020-26956-3，XSS 通过粘贴和剪贴板 API 和 SVG + 图像 onerror 处理程序,在粘贴时对 Firefox，剪贴板 API 内容清理进行模糊测试时<svg><style><image href=1onerror=alert(document.domain)>,当用户从恶意网站复制，然后粘贴内容时，XSS 将执行,引起浏览器和系统崩溃
- CVE-2020-26957， Fenix 目前没有办法撤销错误颁发或恶意的证书
- CVE-2020-26958，nsIContentPolicy::TYPE_INTERNAL_SCRIPT 的内部负载类型创建 HTTP 通道，HTTP 通道类型使用 nsIContentPolicy::TYPE_SCRIPT 的外部内容策略，即

- CVE-2020-26959，ContentParent::RecvInitStreamFilter 堆使用后释放,对 ContentParent IPC 进行模糊测试时，导致了程序崩溃
- CVE-2020-26960， nsTArray 调用 Compact 将导致 JS_GC 中的 use-after-free 错误
- CVE-2020-26961，RFC1918 使用 IPv4 映射地址绕过保护，将 Firefox 与 Trusted Recursive Resolver(TRR) 一起使用,这种保护可以防止对位于 LAN 上的机器的基于浏览器的攻击，例如 DNS 重新绑定攻击。但是可以通过使用 IPv4 映射的 IPV6 地址绕过此保护（例如::ffff:192.168.1.254）。导致局域网的机器被攻击
- CVE-2020-26965，浏览器运行下面脚本，有 50%的概率，导致浏览器崩溃，
- CVE-2020-26965， 软键盘将 <input type=password> 更改为 <input type=text>会导致软件键盘类型更改为非密码样式
- CVE-2020-26967，mutation observers 的屏幕截图异常，原因是 kaisersoze，WIP 以获取屏幕截图错误
- 修复编译的配置文件地址，当构建 firefox 时候，rust 版本>=1.48 时候，会导致 Sandboxcrashes，这两个补丁修复此问题。
- CVE-2022-25236 ，Expat 是一款使用 C 语言编写的快速流式 XML 解析器。Expat（又名 libexpat）2.4.5 之前存在代码注入漏洞，该漏洞源于 xmltok_impl.c 缺少某些编码验证，例如检查 UTF-8 字符在特定上下文中是否有效，

- CVE-2022-25315 ，Expat 是一款使用 C 语言编写的快速流式 XML 解析器。在 2.4.5 之前的 Expat（又名 libexpat）中，storeRawNames 中存在整数溢出。
- CVE-2022-40674 ，2.4.9 之前的 libexpat 在 xmlparse.c 的 doContent 函数中有一个 use-after-free 漏洞
- CVE-2023-23606 ，Mozilla 开发人员和 Mozilla Fuzzing 团队报告了 Firefox108 中存在的内存安全漏洞。其中一些 bug 显示了内存损坏的证据，我们认为只要付出足够的努力，其中一些 bug 可能被利用来运行任意代码。
- 解决字体显示的堆栈溢出问题
- CVE-2022-22755 ，通过使用 XSL 转换，恶意 Web 服务器可以向用户提供 XSL 文档，该文档即使在选项卡关闭后仍会继续执行 JavaScript（在同源策略的范围内）。此漏洞影响 Firefox < 97。
- CVE-2022-43680 ，在 libexpat 到 2.4.9 中，由于在内存不足的情况下过度破坏 XML_ExternalEntityParserCreate 中的共享 DTD，会导致释放后使用。firefox 中包含 libexpat 模块代码，受影响。
- CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827
- CVE-2023-4863 ，低于 116.0.5845.187 和 libwebp 1.3.2 的 Google Chrome 中的 libwebp 中存在堆缓冲区溢出，允许远程攻击者通过构建的 HTML 页面执行越界内存写入。（Chromium 安全严重性：严重）
- CVE-2023-5217 ，在低于 117.0.5938.132 和 libvpx 1.13.1 的 Go

ogle Chrome 和 firefox 中，libvpx 的 vp8 编码中存在堆缓冲区溢出，允许远程攻击者通过构建的 HTML 页面潜在地利用堆损坏。（安全严重性：高）

- CVE-2023-7104，在 SQLite SQLite3 3.43.0 及之前版本中发现一个漏洞，该漏洞被分类为严重漏洞。此漏洞会影响功能 sessionReadRecord 文件 ext/session/sqlite3session.c 的组件 make alltest Handler。该操作会导致基于堆的缓冲区溢出。

8.94. fluidsynth：

- CVE-2021-21417,

8.95. fontforge：

- 修复地名错误

8.96. freeradius：

- CVE-2022-41860: 在 freeradius 中，当 EAP-SIM 请求者发送未知的 SIM 选项时，服务器将尝试在内部字典中查找该选项
- CVE-2022-41861: 恶意的 RADIUS 客户端或主服务器可能发送格式错误的 abinary 属性，从而导致服务器崩溃。

8.97. freerdp：

- CVE-2022-39320，在太窄的类型上尝试整数相加，导致分配的缓冲区太小，无法保存写入的数据
- CVE-2022-39317，在 ZGFX 解码器中缺少输入偏移索引的范围检查
- CVE-2022-39316，ZGFX 解码器组件中有一个超出限制的读取
- CVE-2022-39318，
- CVE-2022-39319
- CVE-2022-39347
- CVE-2022-41877
- CVE-2022-39282
- CVE-2022-24882
- CVE-2022-24883

8.98. freetype：

- CVE-2022-27404， 函数 sfnt_init_face 被发现包含堆缓冲区溢出。
- CVE-2022-27405， 函数 FNT_Size_Request 发现 FreeType 提交包含分段违规。
- CVE-2022-27406， FT_Request_Size 包含分段违规。
- CVE-2023-2004，在 src/truetype/ttgxvar.c 的 tt_hvadvance_adjust（）函数的 Freetype 中存在整数溢出漏洞。

8.99. fuse3：

- 修复在 fuse_session_loop_remember 函数中对 poll 函数返回值的错误处理；
- 修复在使用 clone_fd 时可能出现的文件描述符泄漏问题；
- 修复潜在的使用释放后内存的问题,在重新分配内存后重新计算指针的位置。

8.100. future：

- CVE-2022-40899， 允许远程攻击者通过来自恶意 Web 服务器的精心制作的 Set-Cookie 标头导致拒绝服务。

8.101. gcc：

- CVE-2023-4039，保护栈上已保存的寄存器值不被改写
- 修复 goto 语句预测分支，优化中间表示 dump 显示
- 修复 longbranch 测试用例。
- 解决 gcc -std=c++17 在 class 嵌套的构建函数调用报错。

8.102. gdbm：

- 修复执行 gdbm_dump --usage 命令导致栈溢出问题
- 修复 gdbmtool 使用 import 参数时错误，更改读取位置。
- 修复 gdbm_dump 指定-H 参数值为无效字符串时不报错。
- 修复 gdbm_load -r 的问题，改进 gdbmload 中-u 的处理。

8.103. gdb：

- CVE-2023-39130
- CVE-2023-39129
- CVE-2023-39128
- 修复挂载运行进程时的卡死问题

8.104. gdk-pixbuf2：

- CVE-2021-20240，加载精心制作的 GIF 图像时，可能会出现整数溢出导致写入越界。攻击者可能会使应用程序崩溃或可能在受害者系统上执行代码。
- CVE-2020-29385，2.42.2 之前的 GNOME gdk-pixbuf 在函数 write_indexes/lzw.c 中存在拒绝服务（无限循环）。
- CVE-2021-46829，合成或清除 GIF 文件中的帧时允许基于堆的缓冲区溢出，如 io-gif-animation.c composite_frame 所示。这种溢出是可控的，并且可能被滥用于代码执行，尤其是在 32 位系统上。
- CVE-2021-44648，当解码 GIF 文件中 lzw 压缩的图像数据流（lzw 最小代码大小等于 12）时，GNOME gdk-pixbuf 2.42.6 容易受到堆缓冲区溢出漏洞的影响。

8.105. ghostscript：

- CVE-2023-43115

- CVE-2023-36664
- CVE-2023-28879
- CVE-2023-38559

8.106. giflib：

- CVE-2022-28506，gif2rgb.c:298:45 中的 GIFLIB 5.2.1 函数 DumpScreen2RGB()中存在堆缓冲区溢出。
- CVE-2023-39742，通过组件 getarg.c 发现 givlib v.2.1 包含一个分段错误

8.107. git：

- CVE-2022-39260："git shell"命令的参数长度过长可能会导致"split_cmdline()"函数数据溢出，存在任意堆写入和远程执行代码的安全风险。
- CVE-2022-23521：解析.gitattributes 文件时，当存在大量路径模式、单个模式的大量属性或声明的属性名称巨大时，可能会发生多个整数溢出。这种整数溢出会导致任意堆读取和写入，这可能会导致远程代码执行。
- CVE-2022-41903：pretty.c::format_and_pad_commit() 中存在整数溢出。这种整数溢出会导致任意堆写入，这可能会导致任意代码执行。

8.108. glib2：

- 修复 SVACE 静态代码分析器发现内存分配相关问题

- 修复已关闭的应用程序仍然标记为已注册，即使其实现已被销毁
- 修复在错误路径中出现参数泄漏问题。
- 修复 g_open 失败时出现内存泄漏问题。
- 修复由代码逻辑问题引入的无效输入的字符串泄漏
- 修复长域名导致的缓冲区溢出问题
- 修复如果配置了不正确的 socks 代理，这可能会导致无限循环问题
- 修复线程销毁过程中的内存泄漏。
- 修复在调用到 g_get_user_database_entry 中出现段错误
- 修复 TYPE_CHECK 失败时出现内存泄漏问题
- 修复语言设置为繁体时，部分组件显示英文问题

8.109. glibc：

- CVE-2023-5156 ，2023-4806 的修复引入了内存泄漏的可能性，这可能会导致应用程序崩溃
- CVE-2023-4806，在极少数情况下，getaddrinfo 函数可能会访问已释放的内存，从而导致应用程序崩溃。
- CVE-2023-4813，在不常见的情况下，gaih_inet 函数可能会使用已释放的内存，从而导致应用程序崩溃。仅当调用 getaddrinfo 函数并且/etc/nsswitch.conf 中的主机数据库配置为 SUCCESS=continue 或 SUCCESS=merge 时，此问题才可被利用
- 修复在使用 gprof 或是其它跟踪函数调用轨迹的程序时可能会出来内存越

界而造成程序崩溃的场景。

- 修复使用 LD_AUDIT 时，可能会产生 core 的问题。

8.110. glusterfs：

- 修复 timer.c 中 event 可能出现的 coredump
- CVE-2022-48340
- 修复 upcall-internal 打印的非预期 linked_inode 的地址;
- 修复使用 [..] 来匹配模式的错误;
- CVE-2023-26253

8.111. gnome-user-docs：

- 修复索引页面文件中的信息错误;
- 修复键盘、文件、硬件、鼠标等页面中的用户文档信息错误;
- 修复音乐、网络等页面中的用户文档信息错误;
- 修复电源、打印、会话、声音等页面中的用户文档信息错误;

8.112. gnulib：

- CVE-2018-17942

8.113. gnupg2：

- CVE-2022-34903

8.114. gnuplot：

- CVE-2020-25969

8.115. gnutls：

- CVE-2022-2509，由于 gnutls_pkcs7_verify 函数在验证 pkcs7 签名时出现双 free 错误。
- CVE-2021-4209，NULL 指针解引用缺陷
- CVE-2023-0361，RSA ClientKeyExchange 消息处理中的定时侧通道。这个侧信道足以在 Bleichenbacher 式攻击中通过网络恢复 RSA 密文中加密的密钥
- CVE-2023-5981，RSA-PSK ClientKeyExchange 中对畸形密文的响应时间与使用正确 PKCS#1 v1.5 填充的密文的响应时间不同的漏洞

8.116. golang：

- CVE-2023-24539，html/template: 对 CSS 值处理不当。当插入到 CSS 上下文中时，尖括号（<>）不被认为是危险字符。包含由 '/'字符分隔的多个操作的模板可能导致意外关闭 CSS 上下文，并允许在不受信任的输入下注入意外的 HTML 代码。
- CVE-2023-24540，html/template: 对 JavaScript 空格处理不当。并非所有有效的 JavaScript 空白字符都被认为是空白。在 JavaScript 上下文中，包含字符集"\t\n\f\r\u0020\u2028\u2029" 之外的空白字符的模板，

在执行期间可能无法正确清理。

- CVE-2023-29400，html/template: 对 HTML 空属性处理不当。在未加引号的 HTML 属性中包含 actions 的模板（例如:"attr={{.}}"）在空输入下执行可能会导致在解析 HTML 规范化规则时产生意外结果。这可能允许在标记中注入任意 attributes。
- CVE-2023-29402，当使用 cgo 时，go 命令在构建时可能会生成意外的代码。这可能导致在运行使用 cgo 的 go 程序时出现意外行为。当运行包含目录名称中带有换行符的不受信任的模块时，可能会发生这种情况。
- CVE-2023-29403，在 Unix 平台上，当以 setuid/setgid 位运行二进制文件时，Go 运行时不会有任何不同的行为。在某些情况下，这可能是危险的，比如在转储内存状态或者假设标准输入/输出文件描述符的状态时。如果以 setuid/setgid 方式执行的二进制文件在标准输入/输出文件描述符关闭的情况下进行文件打开操作，可能会导致使用提升的权限读取或写入意外的内容。类似地，如果以 setuid/setgid 方式运行的程序因发生 panic 或接收到信号而被终止，可能会泄漏其寄存器的内容。
- CVE-2023-29404，当使用 cgo 时，Go 命令可能会在构建时执行任意代码。
- CVE-2023-29405，go 命令在使用 cgo 时可能会在构建时执行任意代码。这可能发生在对恶意模块运行"go get"或运行构建不受信任代码的任何其他命令时。
- CVE-2023-29406，HTTP/1 的客户端并没有完全验证 Host 头的内容。恶

意构造的 Host 头可以注入额外的头部或整个请求。通过修复，HTTP/1 的客户端现在拒绝发送包含无效的 Request.Host 或 Request.URL.Host 数值的请求。

- CVE-2023-29409，在证书链中使用极大的 RSA 密钥可能导致客户端/服务器在验证签名时消耗大量的 CPU 时间。
- CVE-2023-39318，html/template 包在<script>上下文中不能正确处理类似 HTML ""注释标记和 hashbang "#!"注释标记。这可能导致模板解析器错误地解释<script>上下文中的内容，从而使动作不正确地被转义。这可能被利用来进行 XSS 攻击。
- CVE-2023-39319，html/template 包没有正确地处理<script>上下文中 JS 文字中的"<script"、"<!--"和"</script"出现的规则。这可能导致模板解析器错误地认为脚本上下文被提前终止，从而使动作不正确地被转义。这可以被利用来进行 XSS 攻击。
- CVE-2023-39323，行指令（“//line”）可以用于绕过对“//go:cgo_”指令的限制，允许在编译过程中传递被阻止的链接器和编译器标志。这可能会导致在运行“go build”时意外执行任意代码。行指令需要指令所在文件的绝对路径，这使得利用此问题变得更加复杂。
- CVE-2023-39325，恶意的 HTTP/2 客户端可以通过快速创建请求并立即重置它们来导致服务器消耗过多的资源。
- CVE-2023-39326，恶意 HTTP 发送方可以使用分块扩展，导致接收方从网络中读取的请求或响应正文字节数比正文字节数多得多。

- CVE-2022-24921
- CVE-2022-23773
- CVE-2022-28327
- CVE-2022-24675
- CVE-2021-44717
- CVE-2022-32148
- CVE-2022-1962
- CVE-2022-1705
- CVE-2022-30633
- CVE-2022-30635
- CVE-2022-30632
- CVE-2022-28131
- CVE-2022-30631
- CVE-2022-30629
- CVE-2022-30634
- CVE-2022-32189
- CVE-2022-29804
- CVE-2022-29526
- CVE-2022-27664
- CVE-2022-41715
- CVE-2022-2880
- CVE-2022-2879
- CVE-2022-41716
- CVE-2022-41717
- CVE-2022-41723
- CVE-2022-41724
- CVE-2022-41725
- CVE-2023-24534

- CVE-2023-24536
- CVE-2023-24537
- CVE-2023-24538
- 修复 rpm 重复提供文件问题：移除 golang-help 子包内的不必要文件，如共享库。
- 修复重启 docker 服务低概率卡住问题：运行时修改，使用原子序数持续访问 pollDesc r/w Gs。
- 修复概率性出现 docker 进程卡死问题：不要在 tracebackothers 中使用 allglock，封装对 allgs 的访问，解决接收信号时的死锁问题。
- CVE-2023-45285，测试用例不适用所在 go 版本的问题：修改测试用例，使用国内 goproxy 代理，测试结果预计输出改为 1.15 版本内容。

8.117. google-gson：

- CVE-2022-25647： 源于 writeReplace()方法反序列化不受信任的数据，可导致 DoS 攻击。

8.118. gpm：

- systemd 读取 PIDFile 的时候，服务主(daemon)进程可能还未将 PID 写入到 PID 文件中或写入未完成，这时 systemd 读取时将出现问题。解决方案：在服务启动后让 systemd 延时读取 PIDFile

8.119. grep：

- 修复使用非 ASCII utf-8 字符进行 grep 时输出错误的问题

8.120. grpc：

- CVE-2023-4785：gRPC 中的 TCP 服务器缺乏错误处理

8.121. grub2：

- CVE-2021-3981，它的配置文件 grub.cfg 是使用错误的权限集创建的，允许非特权用户读取其内容。用户最终可以读取 grub.cfg 中存在的任何加密密码，可能会对数据机密性产生影响
- CVE-2021-3697，某些 1px 宽度的图像可能导致在 grub_jpeg_ycrcb_to_rgb()函数中往野指针写入数据
- CVE-2022-28735，
- CVE-2022-28736，在执行引导之前，若多次调用 grub_cmd_chainloader()函数会触发的 use-after-free 错误
- CVE-2022-28734，拆分 head 的代码总是将指针提前到行尾,而处理未拆分标头的代码不会将指针提前。攻击者控制的数据包集可能会导致 grub_mm_region 结构中 current_line 缓冲区之后的“next”指针的第一个字节归零
- CVE-2022-28733，收包含无效 IP 碎片信息的数据包时，可能造成 rsm->total_len 数据溢出
- CVE-2021-3695 ，在处理没有 alpha 的 16 位灰度 PNG 图片时，可能发

生内存越界写入

- CVE-2021-3696，击者通过精心制作的 PNG 图像利用该漏洞导致哈夫曼表处理时的越界写入
- CVE-2022-2601，grub_font_construct_glyph（）中的缓冲区溢出可能导致越界写入和可能的安全引导绕过
- CVE-2022-3775，呈现某些 unicode 序列时，无法正确验证字体宽度和高度。这些值进一步用于访问字体缓冲区，从而可能导致越界写入
- CVE-2023-4692， grub2 的 NTFS 文件系统驱动程序中存在越界写入缺陷
- CVE-2023-4693， grub2 的 NTFS 文件系统驱动程序中存在越界读取缺陷
- 修复 grub-core/loader/multiboot_elfxx.c 文件中内存泄漏
- 在 grub-core/normal/cmdline.c 中，修复两个相关的整数下溢
- 在 grub-core/fs/iso9660.c 中修复 grub_iso9660_susp_iterate()函数中的内存泄漏
- 在 grub-core/fs/squash4.c 中修复 grub_squash_iterate_dir()函数中的内存泄漏
- 在 grub-core/fs/xfs.c 中修复 XFS 模块的内存泄漏
- 在 grub-core/kern/file.c 文件中修复 grub_file_open()函数中的错误处理
- 在 grub-core/kern/fs.c 文件中，修复在 i386-pc 模式下的大分区可能的整数溢出

8.122. gssntlmssp：

- CVE-2023-25567，GSS-NTLMSSP 在解码目标信息时，它具有越界读取
- CVE-2023-25564， 变量 outlen 未初始化，可能导致写入零
- CVE-2023-25563，32 位整数溢出条件可能导致对的错误检查内部缓冲区长度的一致性。这会导致 DoS 因为服务可能最终从未映射的内存中读取并崩溃
- CVE-2023-25565， 错误条件错误地假定 cb 和 sh 缓冲区会包含需要释放的数据的副本

8.123. gstreamer1-plugins-good：

- CVE-2022-2122，qtdemux 元素中的整数溢出 qtdemux_inflate 这会导致段错误，或者可能导致堆覆盖
- CVE-2022-1920 ，gst_matroska_demux_add_wvpk_header 函数中 matroskademux 元素中的整数溢出，允许在解析 matroska 文件时进行堆覆盖
- CVE-2022-2121，avidemux 元素中的整数溢出 gst_avi_demux_invert 允许在解析 avi 文件时进行堆覆盖
- CVE-2022-1922，matroskademux 元素中的整数溢出 gst_matroska_decompress_data 这会导致段错误，或者可能导致堆覆盖
- CVE-2022-1923， matroskademux 元素中的整数溢出 gst_matroska

_decompress_data 这会导致段错误，或者可能导致堆覆盖

- CVE-2022-1924， matroskademux 元素中的整数溢出 gst_matroska _decompress_data 这会导致段错误，或者可能导致堆覆盖
- CVE-2022-1925， matroskademux 元素中的整数溢出 gst_matroska _decompress_data 这会导致段错误，或者可能导致堆覆盖
- CVE-2021-3497 ，
- CVE-2021-3498

8.124. gtk3：

- 修复中文繁体、简体表述问题

8.125. gtk-doc：

- 修复 gtkdoc-rebase --aggressive 执行命令报错

8.126. guava20：

- CVE-2023-2976，允许计算机上有权访问默认 Java 临时目录的其他用户和应用程序访问 FileBackedOutputStream 中创建的文件

8.127. guava：

- CVE-2023-2976，FileBackedOutputStream 类使用 Java 的默认临时目录创建文件，由于创建的文件名容易被攻击者猜测，允许具有访问默认 Jav

a 临时目录权限的攻击者可创建同名的恶意文件造成文件冲突，破坏应用程序的正常功能

8.128. gvfs：

- 修复 gvfs 因 update_fstab_volumes ()引起的内存泄漏问题
- 修复多处内存泄露

8.129. haproxy：

- CVE-2023-25725
- CVE-2023-0056
- CVE-2023-40225
- CVE-2023-0836
- CVE-2023-45539

8.130. harfbuzz：

- CVE-2022-33068,
- CVE-2023-25193

8.131. hdf5：

- CVE-2018-13867： H5Faccum.c 中的函数 H5F__accum_read 存在读越界。

- CVE-2018-14031：H5T.c 中的函数 H5T_copy 中存在 heap-based buffer over-read。
- CVE-2018-16438，在 H5Lexternal.c 的 H5L_extern_query 中存在越界读取。
- CVE-2019-8396，H5Olayout.c 中的 H5O__layout_encode 中的缓冲区溢出允许攻击者通过精心制作的 HDF5 文件造成拒绝服务。此问题是在重新打包 HDF5 文件时触发的，也称为“大小 2 的无效写入”。
- CVE-2020-10812，位于 H5Fquery.c 中的函数 H5F_get_nrefs（） 中存在空指针取消引用。它允许攻击者造成拒绝服务。
- CVE-2021-37501：HDFGroup hdf5-h5dump 1.12.0 到 1.13.0 中的缓冲区溢出漏洞允许攻击者通过 /hdf5/tools/lib/h5tools_str.c 中的 h5tools_str_sprint 造成拒绝服务。
- CVE-2018-14033，H5Olayout.c 中的 H5O_layout_decode 函数中存在 heap-based buffer over-read，与 HDmemcpy 相关。
- CVE-2018-14460，H5Osdspace.c 中的 H5O_sdspace_decode 函数中存在基于堆的缓冲区溢出。
- CVE-2020-10811，位于 H5Olayout.c 中的函数 H5O__layout_decode() 中存在基于堆的缓冲区过度读取。它允许攻击者造成拒绝服务。
- CVE-2020-10810，位于 H5AC.c 中的函数 H5AC_unpin_entry（） 中存在空指针取消引用。它允许攻击者造成拒绝服务。
- 修复多个命令执行报错

8.132. hdparm：

- 修复打印密码的安全问题。
- 修复 sysfs_write_attr()方法中 fd 不释放问题。
- 修复了 --set-sector-size 和物理/逻辑扇区大小的问题。
- 修正了“hdparm -Istdin”的输出有时会被截断的错误，和尝试从不存在的驱动器读取 LOG 数据的问题。

8.133. hiredis：

- 修复 redisvFormatCommand 中的堆缓冲区溢出问题；
- CVE-2021-32765,
- 修复 mem_size 溢出问题

8.134. httpd：

- CVE-2022-22719,httpd 的 mod_lua 模块在 r:parsebody 中使用未初始化的值，精心设计的请求正文可能会导致对随机内存区域的读取，这可能会导致进程崩溃。
- CVE-2022-22720，HTTP Server 2.4.52 及更早版本在丢弃请求正文时遇到错误时无法关闭入站连接，从而将服务器暴露于 HTTP 请求。
- CVE_2022-22721，如果在 32 位系统上将 LimitXMLRequestBody 设置

为允许大于 350MB（默认为 1M）的请求正文，则会发生整数溢出，随后会导致越界写入。

- CVE-2022-23943，修复 HTTP Server 的 mod_sed 模块存在越界写入风险，该漏洞允许攻击者使用某些特制的数据覆盖正在使用的 mod_sed 的 httpd 实例的内存，并可能对机密性、完整性和可用性造成影响。
- CVE-2022-29404，在 2.4.53 及以下版本的 httpd 存在漏洞可能导致 httpd 拒绝服务，攻击者通过恶意的 lua 请求脚本，携带无限制的请求体进行请求，导致资源耗尽，httpd 拒绝服务；httpd 没有针对请求体大小进行限制。
- CVE-2022-30556,在 2.4.53 及以下版本的 httpd 可能会向 lua_websocket_read 函数调用者返回缓冲区以外内存的数据，导致信息泄露;
- CVE-2022-28614，在 2.4.53 及以下版本的 httpd 中 ap_rputs 输入异常时，调用 ap_write 函数后可能会读取意外内存信息；
- CVE-2022-26377，在 2.4.53 及以下版本的 httpd 存在当 mod_proxy_ajp 中格式错误或异常的 HTTP 请求被用户和 Web 服务器之间的数据流中的一个或多个实体（例如代理或防火墙）解释时，它们可能会被不一致地解释，从而在其他设备不知道的情况下允许攻击者将请求走到另外设备，构造 ajp 请求头中存在 Transfer-Encoding，但值不为 chunked，将会绕过判断，到达另一分支进行处理请求；
- CVE-2022-30522，在 2.4.53 及以下版本的 httpd 存在 httpd 若配置在 mod_sed 中进行上下文转换时，由于 mod_sed 分配内存无限制，可能导

致 httpd 服务由于内存不足的情况而崩溃，或者消耗系统上的大量内存，在使用 mod_sed 进行上下文进行转换时，使用异常大的输入；

- CVE-2022-28615，在 2.4.53 及以下版本的 httpd 存在 ap_strcmp_match 函数读取超过字符串入参长度的漏洞，攻击者用 lua 脚本调用该接口传入超长字符串参数，字符串数组下标读取超出范围导致 httpd 服务崩溃；
- CVE-2022-31813，在 2.4.53 及以下版本的 httpd 存在使用代理时，可能不会基于客户端的首部逐跳机制，把 X-Forwarded-For 字段信息发送到源服务器，这可用于跳过源服务器基于 IP 的身份验证，通过构造伪 X-Forwarded-For 字段信息，访问源服务器，因为真正 X-Forwarded-For 字段信息无法发送到源服务器，源服务器无法基于 X-Forwarded-For 字段中 ip 对客户端信息进行身份验证；
- CVE-2022-28330，在 2.4.53 及以下版本的 httpd，window 平台下配置 mod_isapi 处理请求，从 URL 获取请求文件名时，判断文件名字符串后一位是否为“/”，可能存在访问越界的问题;
- CVE-2022-36760，当 mod_proxy_ajp 中格式错误或异常的 HTTP 请求被用户和 Web 服务器之间的数据流中的一个或多个实体（例如代理或防火墙）解释时，它们可能会被不一致地解释，从而在其他设备不知道的情况下允许攻击者将请求走到另外设备；
- CVE-2006-20001,通过设置传入标头中“If”的值，使得 mod_dav 在解析时越界或写入 0 字节，继而导致 httpd 服务崩溃;
- CVE-2022-37436，mod_proxy 处理响应标头时如果处理不正确，可能导

致 httpd 服务存在安全风险，恶意后端使用 mod_proxy 对 httpd 响应标头提前拆分，导致部分标头合并到响应正文中，如果合并的部分标头存在恶意安全目的，则导致 httpd 服务有安全问题；

- 修复 htcacheclean 启动时的会提示错误消息；
- CVE-2023-25690，当 mod_proxy 与某种形式的 RewriteRule 或 ProxyPassMatch 一起启用时，配置会受到影响;
- CVE-2023-27522，Apache HTTP Server 中通过 mod_proxy_uwsgi 存在 HTTP 响应走私漏洞;
- CVE-2019-17567，Apache HTTP Server 版本 2.4.6 到 2.4.46 mod_proxy_wstunnel 配置在一个不一定由源服务器升级的 URL 上，无论如何都会对整个连接进行隧道传输，从而允许同一连接上的后续请求在没有 HTTP 验证、身份验证的情况下通过或授权可能配置。
- CVE-2023-31122，httpd 的配置文件中使用 mod_macro 进行宏定义，且宏的字符串超长（大于最大值 8192bit）时，存在越界读写的问题，导致服务数据泄露。
- CVE-2023-45802，当客户端重置 HTTP/2 流（RST 帧）时，有一个时间窗口，如果请求的内存资源没有立即回收。相反，取消分配被推迟到连接关闭。客户端可以发送新的请求和重置，使连接保持繁忙和打开，并导致内存占用率不断增长。连接关闭时，所有资源都被回收，但在那之前，进程可能会耗尽内存。

8.135. hyperscan：

- CVE-2022-29486， Hyperscan 库中存在不适当的缓冲区限制，这可能会允许未经身份验证的用户通过网络访问升级权限。
- CVE-2023-28711， Hyperscan 库中控制流管理不足可能会允许经过身份验证的用户通过本地访问潜在地启用拒绝服务。

8.136. ibus-typing-booster：

- 修复中文表述错误

8.137. icu：

- 修复中文表述错误

8.138. ImageMagick：

- CVE-2022-1115
- CVE-2022-3213
- CVE-2022-32547
- CVE-2022-44267
- CVE-2022-44268
- CVE-2023-1289
- CVE-2023-1906
- CVE-2023-34151
- CVE-2023-3428

- CVE-2023-39978

8.139. indent：

- CVE-2023-40305，解析一个包含特殊构造的大括号序列的文件时，该函数可能超出为其分配的内存缓冲区的大小

8.140. initial-setup：

- 还原“修复 DBus 启动器的导入”。
- 修复重新配置模式检测中的拼写错误。
- 修复 DBus 启动器的导入 。
- 修复 DBus 启动器的导入。
- 修复 initial-setup.service 启动失败报错问题：initial-setup 版本太旧，与 anaconda 版本不匹配，需要升级。
- 修复 Makefile 中的 Zanata 客户端检测 。
- 修复 Zanata CLI 调用中的错字 。
- 修复 Zanata CLI 调用中的错字。

8.141. initscripts：

- 解决软件包重复提供文件 rc.local 导致的升级过程中文件冲突问题；

- 解决 resolv.conf 被清空的问题

8.142. intel-sgx-ssl：

- CVE-2022-2068,c_rehash 脚本未正确地清除 shell 元字符以防止命令注入的其他情况，
- CVE-2022-0778，BN_mod_sqrt 函数在某些情况下，对于非素数 p，计算无法完成，可能导致无限循环
- CVE-2022-1292，没有正确地对 shell 元字符进行处理，以防止命令注入
- CVE-2022-2097，AES OCB 模式的实现中存在一个错误，导致在进行加密/解密时，最后一个 96 字节块的最后一个 16 字节块被完全遗漏

8.143. iperf3：

- CVE-2023-38403，通过特制的长度字段导致整数溢出和堆损坏

8.144. ipmitool：

- 修复了 alert 标记位和 ipmi 规定不符的部分
- 修复 msg 负载长度没有随 payload_length 的更新而更新
- 解决时间戳和时区相关问题

8.145. iproute：

- 修复无法获取内核 diffserv 参数的问题
- 修复 fdb get 命令导致的内存泄露问题
- 修复 devlink 命令缺少参数时执行失败的问题
- 修复 ip addr show 导致内存泄露问题
- 修复 udp6 统计信息错误问题
- 修复内存拷贝过程中，长度解析错误问题
- 使用动态获取/proc 目录的方式修复 netns 配置失败的问题
- 修复 vlan 模式展示错误问题

8.146. ipset：

- 修复 ipset list -o xml 偶发输出异常问题

8.147. iputils：

- 修复 ping6 绑定到 VRF 和地址的问题
- 修复当只指定地址（没有 VRF）时出现的权限问题，除非具有 CAP_NET_ADMIN（即 root）权限。
- 修复 AX.25 和 NETROM 的 ARP 协议字段

8.148. ipxe：

- 修复避免分配失败时的死循环问题。
- 修复 ipxe 使用相对 url 引导时，类似这样的 url：/foo/bar/<some mac

- 修复 pci 读取配置初始化所有字段失败问题。
- 修复嵌入式设备在使用 ipxe 从 ftp 服务引导加载镜像时，会下载文件失败问题；
- 添加宏 enable_i386 来控制是否编译 i386 架构相关内容、解决安装 ipxe-roms 缺少依赖问题

8.149. iso-codes：

- 修正一些翻译错误

8.150. iSulad：

- 修复当 load 镜像时 uid/gid 设置错误问题
- 修复 isulad-shim 命令 encoding 问题。
- 修复 utils 模块 encoding 问题。
- 修复输入模块的编码不规范问题。
- 修复获取网络命名空间路径检测。
- 修复当标准输出为 false 时 cri attach 问题。
- 修复 cpu-quota 设置为-1 时超出范围问题。
- 修复 exec_request_to_rest 中忘记处理 suffix 问题。
- 修复 session 内存泄露问题。
- 解决 json-confs 在默认运行时和 cri 运行时后非法释放问题。
- 修复 uwait 可能在释放后被使用问题。

- 针对 websocket 接收数据过长的错误修复。
- CVE-2022-36109，将主组加入附加组。
- 修复为执行用户增加额外 gids。
- 解决 bug 关于创建网络插件实例失败后未 unlock m_podsLock 对象问题。
- 修复 isulad-shim 日志丢失 bug。
- 修正无法删除覆盖图层目录下的图层的错误。
- 刷新时无法加载或提取 image 的错误修正。
- 修复重复申请内存错误。
- 修复内存泄漏和数组访问超出边界问题。
- 修复 top_layer 函数内存泄露问题。
- 修复 layer 不完整问题。
- 修复 inspect 以 digest 标记的 image 错误。
- 修复卡死的健康检查阻止容器停止的错误。
- 修复 implicit_digest 问题。
- 修复 exec 时缓冲区溢出问题。
- 修复 memset 问题。
- 修复 api 模块 cmakelist 问题。

8.151. itstool：

- 解决了-o 和--output=无效的问题
- 修复了一个与 Python 3.7 兼容性的问题，不需要将字符串编码为字节。

- 修复了一个 Python 2/3 问题，并添加了一个测试用例。
- 修复了一个关于文件处理的问题。
- 修复了关于 libxml2 内存管理的问题，以更谨慎地处理内存。
- 解决了一个在特定情况下崩溃的问题。。

8.152. jakarta-servlet：

- 解决 jakarta-servlet 和 glassfish-servlet-api 同时安装冲突问题

8.153. java-11-openjdk：

- 修复计算 maxmaxcode 时的整数溢出问题
- 解决 fd 泄露问题
- CVE-2023-22081
- CVE-2023-22006
- CVE-2023-22036
- CVE-2023-22041
- CVE-2023-22044
- CVE-2023-22045
- CVE-2023-22049
- CVE-2023-25193
- CVE-2023-21930
- CVE-2023-21937
- CVE-2023-21938
- CVE-2023-21939
- CVE-2023-21954

- CVE-2023-21967
- CVE-2023-21968
- CVE-2023-21835
- CVE-2023-21843
- CVE-2022-21618
- CVE-2022-21619
- CVE-2022-21626
- CVE-2022-21624
- CVE-2022-21628
- CVE-2022-39399
- CVE-2022-21540
- CVE-2022-21541
- CVE-2022-34169
- CVE-2022-21426
- CVE-2022-21443
- CVE-2022-21434
- CVE-2022-21496
- CVE-2022-21248
- CVE-2022-21283
- CVE-2022-21291
- CVE-2022-21293
- CVE-2022-21294
- CVE-2022-21282
- CVE-2022-21296
- CVE-2022-21299
- CVE-2022-21277
- CVE-2022-21305
- CVE-2022-21340

- CVE-2022-21341
- CVE-2022-21360
- CVE-2022-21365
- CVE-2022-21366
- CVE-2022-21476
- JDK-8308884：修复了在执行 GregorianCalender.computeTime()方法时导致 JVM 崩溃的问题。之前的修复增加了崩溃的可能性，现在该修复已在 JDK 11.0.20 中撤回。
- JDK-8283137：修复了 Windows 上 ProcessBuilder 处理带引号参数的问题。

8.154. java-1.8.0-openjdk：

- CVE-2022-21248
- CVE-2022-21283
- CVE-2022-21293
- CVE-2022-21294
- CVE-2022-21282
- CVE-2022-21296
- CVE-2022-21299
- CVE-2022-21305
- CVE-2022-21340
- CVE-2022-21341
- CVE-2022-21349
- CVE-2022-21360
- CVE-2022-21365

- CVE-2022-21426
- CVE-2022-21434
- CVE-2022-21443
- CVE-2022-21476
- CVE-2022-21496
- CVE-2023-21830
- CVE-2023-21843
- CVE-2023-21930
- CVE-2023-21937
- CVE-2023-21938
- CVE-2023-21939
- CVE-2023-21954
- CVE-2023-21967
- CVE-2023-21968
- CVE-2023-21830
- CVE-2023-21843
- CVE-2023-21930
- CVE-2023-21937
- CVE-2023-21938
- CVE-2023-21939
- CVE-2023-21954
- CVE-2023-21967
- CVE-2023-21968
- CVE-2023-22045
- CVE-2023-22049
- CVE-2023-22067
- CVE-2023-22081
- CVE-2023-22045

- CVE-2023-22049
- CVE-2023-22067
- CVE-2023-22081
- 对 HotSpot 虚拟机进行了一系列的性能优化和稳定性修复，包括改进垃圾回收机制，提高了 Java 应用的运行效率和响应性。
- 修复了 HotSpot 虚拟机中发现的多个安全漏洞，增强了 Java 运行时环境的安全性。

8.155. jetty：

- 修复对 mvn(javax.servlet:servlet-api)的依赖关系问题
- CVE-2019-10241
- CVE-2022-2047
- CVE-2022-2048

8.156. jgit：

- 升级到 5.11.0 版本解决问题：1)由于 apache-sshd 升级导致 jgit 编译失败；2)jar 包的路径没有添加到 jgit 的 classpath 引起 java.lang.NoClassDefFoundError 错误；

8.157. js-jquery：

- 解决了一些安全问题，包括 DOM XSS 攻击和 Prototype Pollution 漏洞等；
- 修复使用常规表格时 width()返回不正确的宽度、jQuery 缓存数据的最大值问题

8.158. jsoncpp：

- 修复 json 解析器在处理单引号时的问题；
- 修复判断字符是否需要转义时，可能导致不同环境下的不一致性的问题；
- 修复 Json::Value 和 nullptr 类型之间的比较问题；
- 修复由于编译器优化而导致的内存没有正确清零问题。

8.159. json-c：

- CVE-2021-32292，在 json_parse.c 文件的 parseit 函数中存在一个堆栈缓冲区溢出漏洞。这个漏洞允许攻击者执行恶意代码。

8.160. json-smart：

- CVE-2023-1370，嵌套太多数组和对象会导致堆栈耗尽（堆栈溢出）并使软件崩溃

8.161. jsoup：

- 升级至 1.14.2-1 版本:解析器错误修复和改进,用于处理粗略的 HTML 和 X

ML 等；提供了简单的请求会话管理、增强的解析健壮性，以及大量其他改进和 bug 修复；

8.162. kata-containers：

- 解决 changelog 扫描暴露问题
- 解决在国产海光架构上不设别 CPU 问题

8.163. kexec-tools：

- CVE-2021-20269，优化 kdumpctl 脚本文件，忽略不推荐使用且无效的 kdump 配置选项；
- 解决了在回退到旧系统调用之前未重置 getopt 的问题；

8.164. kiwi：

- 修复临时目录的清理；

8.165. kmod：

- 修复当我们被来自 modinfo 的特定字段询问时内置模块不能正常工作的问题；
- 文档修复了/etc/run 的优先顺序：正确的顺序是/etc/modprobe.d、/run/modprobe.d、/lib/modprobe.d
- 修复我们用于搜索配置文件的优先级顺序。这个正确的是/etc/run、/usr/l

ocal/lib、/lib，用于两个 modprobe.d 和 depmo.d

- 修复出现引号时的内核命令行解析问题。Grub 破坏了命令行，并将其从'module.option=“val with spaces”'更改为'“module.option=val with space”'。尽管这是一种奇怪的行为，而且 grub 本可以被修复，但内核对内置模块的理解是正确的。因此，更改 libkmod 也可以正确解析它。这也带来了内核的另一个隐藏行为：内核命令行中的换行符也是允许的，可以用来分隔选项。
- 修复错误路径上的内存泄漏、溢出和双重释放；
- 修复 kmod_module_get_info（）返回值的文档：我们返回添加到列表中的条目数
- 修复 modules.builtin.alias.bin 索引的输出：由于滥用 kmod_module_get_info（），我们正在写入一个空文件；
- 修复一些内存泄漏；
- 修复 0 长度的内置.alias.bin：至少需要索引头；

8.166. krb5：

- CVE-2023-36054,经过身份验证的攻击者可以通过释放未初始化的指针来导致 kadmind 进程崩溃
- CVE-2022-42898

8.167. ksh：

- 修复只安装 ksh 主包时系统存在空链接文件的问题
- 修复未找到内置路径的问题
- 修复命令历史记录不起作用的问题
- 修复无法获得交互式受限 shell 的问题
- 修复在 ksb 交互式 shell 中，键入 typeset -f 或 functions 回车会发生崩溃的问题

8.168. kylin-control-center：

- 修复 root 用户密码更新不对原密码进行校验问题
- 修复切换屏保模式时的崩溃问题
- 修复每次打开控制面板屏保预览都是黑色问题
- 修复相同 UID 用户删除问题
- 修复默认程序设置中网络浏览器显示异常问题
- 修复内存泄漏问题

8.169. kylin-menu：

- 修复 x86 架构服务器桌面点击两次“我的电脑”会出现三个文件夹问题
- 修复点击开始菜单后再点击任务栏的任务，任务窗口不会还原也没有反应问题

8.170. kylin-theme：

- 修复存在空链接文件问题

8.171. langtable：

- 修复地理信息表述错误

8.172. less：

- CVE-2022-46663；影响性分析说明：less -R 应该要执行文件中的命令。但实际上，上下翻页的命令会覆盖中间的命令，使得中间的命令未被执行而是作为内容显示出来

8.173. leveldb：

- 修复 leveldb::InternalKey::Encode 函数中存在断言报错的问题；
- 修复 AcceleratedCRC32C 函数代码中的字节对齐问题；
- 修复 LRUCache 相关函数中变量未初始化使用的问题。

8.174. libabigail：

- 修正了各种打字错误和格式问题，包括输出中的多余空行和缩进问题。
- 修复了模板声明的哈希函数。

- 修正了数组类型和函数名计算中的问题。
- 解决了 abixml 读取中对类型指针的错误比较，命名类的类型定义和数组类型定义的问题。
- abidiff: 修复了关于 abidiff 报告版本不匹配的问题。
- 修复了数个与递归类型定义处理有关的问题。
- 修复了递归类型定义的处理。
- 修复了递归限定和引用类型定义。
- 递归数组类型定义的修复。
- 修复了 .typeid 文件和打字错误，以及一些文档错误。
- 回归测试和错误修复，以及修改了如何打印工具的版本号。
- 修复了在 writers 中一些与类型忽略相关的问题，涉及到函数类型引用、数组子范围类型，以及命名 typedef 的引用。
- 修正了 abidiff 手册中的编号错误。
- 解决了为 kmidiff 生成手册页的问题（Bug 28663）。
- 修正了 IR 中关于规范化类型传播的文档。
- 修正了 DWARF 读取器在设置类大小时的错误。
- 解决了查看无代码段（corpus-less）翻译单元时导致崩溃的问题。
- 修复了虚拟析构函数错误报告为添加/删除的问题。
- 修正了 abidiff 手册中的编号错误。
- 解决了生成 kmidiff 手册页的问题（Bug 28663）。
- 修正了符号表读取器中的替代地址问题。

8.175. libaio：

- 解决非 root 用户编译失败问题

8.176. libarchive：

- CVE-2021-36976
- CVE-2022-36227

8.177. libassuan：

- 修复单元测试中内存泄漏问题

8.178. libcap：

- CVE-2023-2603
- 修复 getpcaps 抓取 PID 的解析错误
- 修复 VFS_CAP_U32 无法确保定义 XATTR_NAME_CAPS 的 bug

8.179. libcgroup：

- 修复配置文件 cgrules.conf 改变后没有在 pam_cgroups 等模块生效的问题

8.180. libconfuse：

- CVE-2022-40320：confuse.c 组件的 cfg_tilde_expand 存在基于堆的缓冲区越界读取

8.181. libdb：

- 修复潜在的无限循环问题；

8.182. libdvdnav：

- 修复坏损 dvd 中 dvdnav_describe_title_chapters 执行导致的程序崩溃

8.183. libdwarf：

- 修复了处理 split-dwarf 时可能导致内存泄漏的 bug；
- 修正了 libdwarf 对 DWARF5 行表头 DW_LNCT 条目的处理；
- CVE-2020-27545，精心制作的无效行表对象可能会导致 libdwarf 解除引用指针，读取预定 .debug_line 部分之外的单字节
- CVE-2020-28163，如果 DWARF5 行表头的路径名的 FORM 无效，则 fi_file_name 字段可能为空，通过 %s 打印它可能会导致引用地址为 0 的内存，从而可能产生分段违规或应用程序崩溃

8.184. libexif：

- 修复因为使用尾递归导致堆栈溢出，所以采用直接循环替换尾递归，解决堆栈溢出问题
- CVE-2020-0452,如果第三方应用程序致远程代码执行程序，使用此库处理图像数
- CVE-2019-9278,用户交互时，出现不需要额外权限升级软件的现象。
- CVE-2020-0181,出现不需要额外执行权限的远程拒绝服务；
- CVE-2020-0198,出现不需要额外执行权限的远程拒绝服务；
- CVE-2020-0093,本地信息泄露，导致户交互无需额外的执行权限

8.185. libfastjson：

- CVE-2020-12762，没有检查传入的文件大小，直接将文件大小×2，而过大的文件长度可能会在×2 时导致整数溢出

8.186. libgcrypt：

- 修复 Elgamal 加密在其他实现中的问题，CVE-2021-33560
- 修复 macOS 上的对齐问题。
- 修复在 "Curve25519" 中的 gcry_pk_get_param 中的中止。
- 修复在使用 gcc-4.7 的 i386 构建中的问题。
- 修复 s390 上 AES 的 OCB 解密中的校验和计算问题。
- 修复与 curve 25519 的 gcry_mpi_ec_add 相关的回归。
- 在 EdDSA 的错误代码路径中修复内存泄漏。

- 在 x86 上使用 --disable-asm 时修复构建问题。
- 在 ECDH 代码中修复内存泄漏。
- 在 SHA2-avx2 中修复超出输入缓冲区末尾的读取。
- 修复 1.9.0 中引入的哈希函数中的可利用漏洞。
- 在 ARMv7 上禁用 NEON 时修复编译错误。
- 修复 KDF 模块中的自检。
- 在 x86 上修复 32 位交叉构建问题。
- 为 SHA512 修复非 NEON ARM 汇编实现。
- 在模块反演实现中修复溢出。
- 对于 AVX/AVX2 实现的 Blake2，修复寄存器访问。
- 在 arm64 上修复 GCM Bug，这会导致 OMEMO 等问题。
- 修复 mpi_copy 以正确处理不透明 MPI 的标志。
- 修复 mpi_cmp 以将 +0 和 -0 视为相同。
- 防范 ECC 时序攻击 CVE-2019-13627。

8.187. libgeotiff：

- 解决工具 geotiff 的提示信息错误问题

8.188. libgovirt：

- 更新 certificates，解决 make check 报错

8.189. libguestfs：

- 撤销外源 supermin.d-x86.tar.gz 和 supermin.d-arm.tar.gz，修改 libguestfs.spec 文件，使 supermin 在编译过程中自动生成，并修复 guestfish 无法找到共享目标文件问题

8.190. libhangul：

- 修复中文表述错误

8.191. libiscsi：

- 修正了 iscsi_create_context 时的内存泄露
- 修正了不检测 malloc 返回值造成的空指针问题
- 修正了调用 iscsi_task_mgnt_lun_reset_async 时的段错误问题
- 修正了 iscsi-inq 的调试级别问题

8.192. libksba：

- CVE-2022-47629：低于 1.6.3 的 Libksba 在 CRL 签名解析器中容易出现整数溢出漏洞。
- CVE-2022-3515：在 Libksba 库中发现一个漏洞，这是 CRL 分析器中的整数溢出所致。

8.193. liblouis：

- CVE-2023-26769：该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 compileTranslationTabel.c 中的 resolveSubtable 函数导致拒绝服务。
- CVE-2022-26981：该漏洞源于 compileTranslationTable.c 中的 compilePassOpcode 存在缓冲区溢出。
- CVE-2022-31783： 该漏洞源于在 compileTranslationTable.c 的 compileRule 中存在越界写入。
- CVE-2023-26767： 该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 logginc.c 端点的 lou_logFile 函数导致拒绝服务。
- CVE-2023-26768： 该漏洞源于存在缓冲区溢出漏洞，远程攻击者利用该漏洞可以通过 compileTranslationTable.c 和 lou_setDataPath 函数造成拒绝服务。

8.194. libmatemixer：

- 修复服务器系统无音频设备情况下.xsession 日志不断报错无限制消耗存储空间问题;

8.195. libmateweather：

- 修复中文表述错误

8.196. libmemcached：

- 修复 memcapable 命令执行报错连接超时

8.197. libmetalink：

- 修复无效字段类型导致的崩溃
- 修复 parser_json 在解析设备时，在 netdev 家族源中不将字符串解析为 map 的判断的 bug.

8.198. libmicrohttpd：

- CVE-2023-27371，当攻击者远程发送恶意 HTTP POST 数据包时，程序内部会出现越界读取和 find_boundary()函数崩溃

8.199. libmpc：

- 解决 karatsuba 精确计算中 0 部分的符号出现差错的问题；

8.200. libmtp：

- 修复 usb 接口读取数据问题

8.201. libpcap：

- 修复 device open 时内存泄漏的问题；

- 修复内核不支持 CONFIG_PACKET_MMAP 时发生段错误问题；
- 修复 DLT_LINUX_SLL 变为 DLT_LINUX_SLL2 时 VLAN 解析错误问题；
- 修复子类型解析错误问题"type XXX subtype YYY"
- 修复 pcap_compile()内存泄漏；
- 修复 pcap_findalldevs()没有按序排列的问题；
- 修复"unknown ether proto 'aarp'"问题；
- CVE-2019-15161
- CVE-2019-15162
- CVE-2019-15163
- CVE-2019-15164
- CVE-2019-15165

8.202. libpfm：

- 修复 libpfm-devel 包安装没有依赖 libpfm 的问题

8.203. libproxy：

- CVE-2020-25219

8.204. librabbitmq：

- CVE-2023-35789

8.205. LibRaw：

- 修复使用makernotes.cpp和misc_parsers.cpp中未初始化的值的问题，
- CVE-2023-1729，该漏洞源于使用函数 raw2image_ex(int) 时存在堆缓冲区溢出。

8.206. libreswan：

- CVE-2023-38710
- CVE-2023-38711
- CVE-2023-38712

8.207. librsvg2：

- CVE-2023-38633，由于处理路径存在逻辑错误，导致攻击者可以传入一个恶意构造的 SVG 图片，进而读取到任意文件

8.208. libselinux：

- 修复 restorecon_xattr 命令参数校验出现 Segmentation fault（core dumped）异常的问题
- 修复内部Sha1Update()函数只处理最大为UINT32_MAX的缓冲区的问题

8.209. libsepol：

- 修复引号字符串中使用\0 导致会使 flex 标记器非常慢的问题
- CVE-2021-36084， 处理 classspermissionset 规则时的 heap-use-after-free
- CVE-2021-36086，
- CVE-2021-36085， 在__cil_verify_classperms 中有一个 use-after-free
- CVE-2021-36087， oss fuzz 发现所用策略导致 cil_tree_get_next_path()中的解引用为空

8.210. libsolv：

- CVE-2021-3200：libsolv 的 src/testcase.c 中的 testcase_read（）中存在基于堆的缓冲区溢出，该溢出漏洞可能导致拒绝服务，威胁系统可用性。
- CVE-2021-44568：libsolv 中存在两个堆溢出漏洞，通过 src/solver.c 中的 resolve_dependencies 函数（第 1940 行和第 1995 行）在决策映射变量中存在两个堆溢出漏洞，这可能导致远程拒绝服务。
- CVE-2021-44569：堆缓冲区 libsolv 存在于 src/solver.c 的 solver_solve 函数中：第 3445 行。
- CVE-2021-44571：libsolv 中存在一个堆溢出漏洞，位于 src/policy.c:第 442 行的 prefer_suggested 函数中。
- CVE-2021-44573：libsolv 中存在两个堆溢出漏洞，位于 src/solver.c 的 resolve_installed 函数中:第 1728 和 1766 行。

- CVE-2021-44574：libsolv 中存在一个堆溢出漏洞，位于 src/solver.c 第 1599 行的 resolve_jobrules 函数中。
- CVE-2021-44575：libsolv 中存在两个堆溢出漏洞，位于 src/solver.c makeruledecisions 函数中:第 147 行和第 307 行。
- CVE-2021-44576：libsolv 中存在两个内存漏洞，位于 src/solver.c 的 resolve_weak 函数中:第 2222 行和第 2249 行。
- CVE-2021-44577：libsolv 中存在两个堆溢出漏洞，src/solver.c 的传播函数中存在错误:第 490 行和第 524 行。
- 修复使用 testsolv 执行案例时的内存泄漏，*resultp 只会保留最后一个循环的指针，会导致内存泄漏；修复使用绑定时解决冲突的段错误；确保在重用求解器时重置

8.211. libspectre：

- 修复格式错误的文档导致的崩溃问题

8.212. libssh：

- CVE-2023-1667，空指针解引用问题，发生在重新协商密钥时进行算法猜测的过程中
- CVE-2023-2283，调用 pki_key_check_hash_compatible 导致返回值发生变化
- 修复在 ssh_userauth_try_publicke 中返回的错误。

- 修复如果通过 opt 设置，客户端不会关闭套接字的 bug。
- 修复 openForward，使其不将 sourcehost 设置为 NULL 的问题。
- 修复 sftp_write 中数据包长度的计算的问题。

8.213. libtar：

- CVE-2021-33643、CVE-2021-33644：使用从 tar 包中的数据作为 malloc 参数，导致 malloc(0)，在后续使用中导致越界读，可能会导致进程崩溃，如果此组件用于外部服务接口提供 zip 解包服务，可能会导致无权限的拒绝服务攻击。
- CVE-2021-33645、CVE-2021-33646：最后一轮读取的 t->th_buf.gnu_longlink 没有释放，存在内存泄露，可导致进程崩溃如果此组件用于外部服务接口提供 zip 解包服务，可能会导致无权限的拒绝服务攻击。

8.214. libtasn1：

- 修复了一些由于非法指针引起的 clang 问题。
- 修复 parser2tree 中的内存泄漏。
- Gtk-doc 修复。
- 修复潜在的由 fscanf 函数引发的缓存区溢出问题。
- 更新 gnulib 文件和许多构建修复程序。
- CVE-2021-46848

8.215. libteam：

- 修复帮助信息中的 options 列表中的—version 选项，将对应的单字符参数 -V 改成了-v。
- 解决在考虑端口时忽略当前状态，存在 100%占用 CPU 的问题

8.216. libtiff：

- CVE-2022-2056
- CVE-2022-2057
- CVE-2022-2058，libtiff/tiffcrop 中的除零错误允许攻击者通过特制的 tiff 文件造成拒绝服务。
- CVE-2022-3597
- CVE-2022-3527，在 LibTIFF/tif_unix 中的_TIFFmemcpy 中有一个越界写入，当从 tools/tiffcrop 调用 extractImageSection 时允许攻击者通过特制的 tiff 文件造成拒绝服务。
- CVE-2022-3526，LibTIFF 4.4.0 在 LibTIFF/tif_unix 中的_TIFFmemset 中有一个越界写入，当从 tools/tiffcrop 调用 processCropSelections 时，允许攻击者通过特制的 tiff 文件造成拒绝服务。
- CVE-2022-3570，tiffcrop 中存在多个堆缓冲区溢出。libtiff4.4.0 中允许攻击者通过特制的 TIFF 图像文件触发不安全或越界内存访问，这可能导致应用程序崩溃、潜在信息泄露或任何其他与上下文相关的影响。

- CVE-2022-3598，libTIFF 4.4.0 在 tools/tiffcrop 中的 extractConting SamplesShifted24 位中有一个越界写入。允许攻击者通过特制的 tiff 文件造成拒绝服务。
- CVE-2022-3599，在 tools/tiffcrop 中的 writeSingleSection 中有一个越界读取，允许攻击者通过特制的 tiff 文件造成拒绝服务。
- CVE-2022-3970，在 LibTIFF 中发现漏洞，这将影响文件 libtiff/tif_getimage.c 的函数 TIFFReadRGBATileExt。操作导致整数溢出。可以远程发起攻击。
- CVE-2022-48281，4.5.0 版本之前的 LibTIFF 中的 tools/tiffcrop.c 中的 processCropSelections 存在基于堆的缓冲区溢出。
- CVE-2023-0795
- CVE-2023-0796
- CVE-2023-0798
- CVE-2023-0799
- CVE-2023-0800
- CVE-2023-0802
- CVE-2023-0803
- CVE-2023-0804，在 tools/tiffcrop.c 中的 tiffcrop 中存在越界读取，允许攻击者通过精心制作的 tiff 文件造成拒绝服务。
- CVE-2023-0797
- CVE-2023-0801，在 libtiff/tif_unix.c 中的 tiffcrop 中有越界读取，允许攻击者导致拒绝-通过制作的 tiff 文件提供服务。
- CVE-2022-48281

- CVE-2023-2731，在 Libtiff/tif_lzw.c 文件中的 Libtiff 的 LZWDecode（）函数中发现 NULL 指针取消引用缺陷。此漏洞使本地攻击者能够处理特定的输入数据，这些数据可能导致程序在解压缩 TIFF 格式文件时取消引用 NULL 指针，从而导致程序崩溃或拒绝服务。
- CVE-2023-26965， LibTIFF 至 4.5.0 中的 tools/tifcrop.c 中的 loadImage（）在通过特制的 TIFF 图像释放后具有基于堆的使用。
- CVE-2023-3316， TIFFClose()中的 NULL 指针取消引用是由于在指定区域时无法打开输出文件（不存在的路径或需要权限（如/dev/NULL）的路径）所致。
- CVE-2023-25433 ， libtiff 4.5.0 容易通过 /libtiff/tools/tiffcrop.c:8499 受到缓冲区溢出的影响。tiffcrop 中的 rotateImage()后缓冲区大小更新不正确会导致堆缓冲区溢出和 SEGV。
- CVE-2023-26966，当 libtiff 读取损坏的小端 TIFF 文件并将输出指定为大端时，libtiff 4.5.0 容易受到 uv_encode()中缓冲区溢出的影响。
- CVE-2023-2908，在 Libtiff 的 tif_dir.c 文件中发现空指针取消引用问题。此问题可能允许攻击者将精心制作的 TIFF 图像文件传递给 tiffcp 实用程序，从而触发运行时错误，从而导致未定义的行为。这将导致应用程序崩溃，最终导致拒绝服务。
- CVE-2023-3576，在 libtiff 中发现漏洞，其中 tools/tifcrop.c 中存在内存泄漏。
- CVE-2023-38288

- CVE-2023-38289，libtiff<=4.5.1 中 raw2tiff.c 中存在多个潜在整数溢出，远程攻击者可以通过特制的 tiff 映像引发基于堆的缓冲区溢出，从而导致拒绝服务（应用程序崩溃）或可能执行任意代码。
- CVE-2023-3618， 在 libtiff 中发现了一个缺陷。由于 libtiff/tif_fax3.c 中 Fax3Encode 函数的缓冲区溢出，特制的 tiff 文件可能会导致段错误，从而导致拒绝服务。
- CVE-2022-40090，4.4.0 之前的函数 TIFFReadDirectory libtiff 中发现了一个问题，允许攻击者通过精心编制的 TIFF 文件造成拒绝服务。
- CVE-2022-34526，在 Tiffsplit v4.4.0 的_TIFFVGetField 函数中发现堆栈溢出。此漏洞允许攻击者通过“tiffsplit”或“tiffcrop”实用程序解析的特制 TIFF 文件导致拒绝服务（DoS）。
- CVE-2023-6228， 在 libtiff 包发布的 tiffcp 实用程序中发现了一个问题。处理构建的 TIFF 文件可能会导致基于堆的缓冲区溢出，从而导致应用程序崩溃。
- CVE-2023-6277，libtiff 存在内存溢出漏洞。向 TIFFOpen() API 传递一个精心构造小于 379 KB 的 tiff 文件可能引发拒绝服务攻击

8.217. libtirpc：

- 修复 fd 锁的内存泄露问题
- 修复使用释放后的内存

- 修复 MT 环境的死锁问题
- 修复 clnt_dg_freeer 的死锁问题
- 修复线程销毁问题

8.218. libvirt：

- 解决由于 libtasn1 升级造成的 libvirt 适配问题
- 修复在 libvirt nwfilter 驱动程序中的锁漏洞,CVE-2022-0897.
- 修复 virsh 命令的中英文翻译问题

8.219. libvncserver：

- 修复了使用 OpenSSL 后端时与 AnonTLS 服务器的加密连接;
- CVE-2020-29260，通过函数 rfbClientCleanup（）发现 libvncclientv 0.9.13 包含内存泄漏

8.220. libwebp：

- CVE-2023-1999，攻击者可以使用 ApplyFiltersAndEncode（）函数并循环通过释放 best.bw 并分配 best=trial 指针。由于 VP8 编码器中的内存不足错误，第二个循环将返回 0，指针仍被分配给试用，AddressSanitizer 将尝试双重释放
- CVE-2023-4863，存在堆缓冲区溢出，远程攻击者可以通过特制的 HTML 页面执行越界内存写入

8.221. libwnck：

- 修复打开浏览器窗口和终端窗口，点击开始菜单后保持开始菜单不消失，再点击任务栏的任务，任务窗口不会还原也没有反应的问题

8.222. libX11：

- CVE-2022-3554，/im/ximcp/imsClbk.c 的函数_XimRegisterIMInstantiateCallback 有内存泄漏。
- CVE-2022-3555， xcb_disp.c 的函数_XFreeX11XCB 结构，对参数 dpy 的操作会导致内存泄漏。
- CVE-2023-3138.X 服务器可以从 XQueryExtension 返回值，这将导致 Xlib 写入超出数组边界的条目来存储它们，尽管这只会覆盖 Displaystruct 的其他部分，而不会超出为该结构分配的边界。
- CVE-2023-43785，_XkbReadKeySyms（）中存在越界内存访问。
- CVE-2023-43786，由于 PutSubImage（）函数中存在无限循环，导致允许本地用户消耗所有可用的系统资源，并拒绝服务。
- CVE-2023-43787，XCreateImage（）中存在整数溢出导致堆溢出。

8.223. libxml2：

- CVE-2023-45322，use-after-free 错误，这个错误仅发生在一个某个内存分析失败时，发生在 tree.c 文件中的 xmlUnlinkNode 中。

- 修复旧的 SAX1 解析器有用户回调相关的错误。
- CVE-2023-28484，解析某些无效的 XSD 模式可能会导致 NULL 指针取消引用，并随后导致 segfault
- CVE-2023-29469，xmlDictComputerFastKey 可能会产生不确定的值，从而导致各种逻辑和内存错误，例如双重空闲
- 修复发生在 xmlStaticCopyNodeList 中的内存泄漏。
- CVE-2022-40303， 在启用 XML_PARSE_HUGE 解析器选项的情况下解析一个千兆字节的 XML 文档时，几个整数计数器可能会溢出。这导致试图以负 2GB 偏移量访问阵列，通常会导致分段故障
- CVE-2022-40304，某些无效的 XML 实体定义可能会损坏哈希表键，从而可能导致后续的逻辑错误。在一种情况下，可以引发 double-free。
- CVE-2016-3709，提交 960f0e2 后，libxml 中可能存在跨站点脚本漏洞
- 修复当 xmlHashAddEntry 失败时在 xmlACatalogAdd 中发生的内存泄漏。
- 修复 xmlACatalogAdd 的内存泄漏。
- CVE-2022-29824，buf.c（xmlBuf*）和 tree.c（xmlBuffer*）中的几个缓冲区处理函数不检查整数溢出。这可能会导致内存写入越界
- CVE-2022-23308，valid.c 在没有 ID 和 IDREF 属性可能会 use-after-free
- 修复由 vagrind 报出的发生在 xmlParseBalancedChunkMemoryRecover 中的错误。

8.224. libXpm：

- CVE-2022-44617，当处理宽度为 0 且高度非常大的图片时，某些解析器函数会被反复调用，并可能导致无限循环
- CVE-2022-46285，解析一个未关闭注释的文件时；文件结束的条件不会被检测到，从而导致无限循环
- CVE-2022-4883，当处理以.Z 或.gz 为扩展名的文件时，该库会调用外部程序来压缩和解压缩文件，并依赖 PATH 环境变量来查找这些程序。这可能会使恶意用户通过操纵 PATH 环境变量来执行其他程序

8.225. libxslt：

- CVE-2021-30560

8.226. libyaml：

- 修复了 yaml_emitter_emit_flow_mapping_key 中的堆缓冲区溢出问题。
- 修复了 yaml-emitter-emit-flow-sequence-item 中的堆缓冲区溢出问题。

8.227. lightdm：

- 修复桌面环境连接 xserver 失败

- 修复缺少 systemd-pam 依赖导致 lightdm.service 启动有报错，且导致 lightdm 无法启动 user 级别的 dbus.service，最终导致用户登录桌面后出现 xfce-polkit 启动报错
- 修复 lightdm 返回的 PAM 消息未翻译的问题
- 修复删除已登录用户后，立即重新创建，出现程序崩溃现象

8.228. linux-sgx：

- CVE-2022-2068 CVE-2022-0778 CVE-2022-1292 CVE-2022-2097

8.229. lksctp-tools：

- libsctp 和 libwithsctp 添加 CURRENT REVISION 和 AGE configure.ac，修复 libsctp 和 libwithsctp 的硬编码版本
- libcnetinet_HEADERS 设置回 sctp.h，修复 netinet/sctp.h 未被安装
- sctp_sendv 接口支持 sendmsg 的信息，修复了 sctp_sendv 上被忽略的参数

8.230. log4j：

- CVE-2021-44832，有权修改日志配置文件的攻击者可以构建恶意配置将 JDBC Appender 与引用 JNDI URI 的数据源一起使用，该 JNDI URI

可以执行远程代码。

- 修复 StrSubstitutor.replace（String，Properties）中输入为 null 时的空指针异常问题。
- 修复 MapLookup 在 DefaultMap 之前查找 MapMessage 的问题。
- 修复检查的缓冲 I/O 在 RollingFileAppenderBuilder 中的逻辑问题。
- 修复 OptionConverter 可能导致 StackOverflow 错误。
- 修复了在属性配置文件中解析筛选器的问题
- 修复 ThreadContextDataInjector 初始化死锁
- 修复 PatternLayout 中的 DefaultConfiguration 泄漏

8.231. logrotate：

- 修复"logrotate 压缩清理日志文件发生错误"的问题
- 修复"在 logrotate 软件包配置文件中，当 prerotate 执行失败时，已备份日志会被重命名"的问题

8.232. lsof：

- 使用管道通信来填充缓冲区为零，修复使用 valgrind 检查代码中存在未初始化的值的问题。
- 修复对于普通文件-Fo 选项打印文件偏移量不起作用的问题。

8.233. lsscsi：

- 修复主机管理的 ZBC 设备不输出它们的大小
- 修复十六进制计数问题，为通用 NVMe 设备提供“-”单线输出，因此“lsscsi -gb”输出是一致的。

8.234. lvm2：

- 修复挂起的 dm 设备缺少 udev 软链接问题。
- 修复当配置文件中 report_command_log 设置为 1 时，命令使用-S|--select 选项时出现的 segfault 问题
- 修复当块设备的物理扇区大小和逻辑扇区大小有差异时创建卷组失败问题

8.235. lxc：

- CVE-2022-47925。
- 修复 lxc 写错误信息函数中转义问题
- 移除进程的 inheritable capability 权限，同时修复了 CVE-2022-24769 安全漏洞
- 修复 ops 为 null 时 coredump 问题
- 修复 isulad 安全挂起函数不能兼容 lxc 挂起函数问题
- 修复 signed 与 unsigned type 类型使用不当的问题,增加 ssize_t 来限制 signed 和 unsigned 类型的最大使用长度。

- 修复 device 路径拼接错误

8.236. m17n-db：

- 修复地名表述问题

8.237. mariadb：

- 修复 ALTER TABLE...ADD PRIMARY KEY 在执行 ADD COLUMN...NULL 后 crash 问题；
- 修复 service_manager_extend_timeout()被调用太频繁问题；
- 修复 ADD COLUMN 时使用太长 DEFAULT 值 Crash 的问题；
- 修复从 MariaDB10.1 或更早版本进行升级的 crash 问题；
- 修复 Multi-pass 恢复时应用一些 redo 日志失败的问题；
- 修复带有 FOREIGN KEY 和 FULLTEXT INDEX 的 RENAME TABLE Crash 问题；
- 空间索引修复
- 虚拟列修复
- Mariabackup 修复
- CVE-2018-3282
- CVE-2016-9843
- CVE-2018-3174
- CVE-2018-3143

- CVE-2018-3156
- CVE-2018-3251
- CVE-2018-3185
- CVE-2018-3277
- CVE-2018-3162
- CVE-2018-3173
- CVE-2018-3200
- CVE-2018-3284
- 修复带有 varchar (utf8)字段索引的堆栈溢出问题；
- 修复 handler::ha_rnd_init(bool)处理带有 InnoDB, joins, AND/OR 条件时的 inited==NONE || (inited==RND && scan)断言问题；
- 修复当 LSN 大于 4G 时, Mariabackup 拷贝加密的 InnoDB 系统表空间失败问题；
- 修复 ALTER TABLE ... FULLTEXT INDEX
- 修复新引入的一些回归错误
- 虚拟列问题修复
- Mariabackup 修复
- InnoDB ALTER TABLE 修复
- InnoDB crash recovery 修复
- Galera crash recovery 修复；
- binlog 修复
- Spider 更新至 3.3.14，修复一些 crash 和结果错误；
- CVE-2019-2510

- CVE-2019-2537
- InnoDB corruption 修复；
- InnoDB purge performance 修复；
- InnoDB ALTER TABLE 修复；
- Galera 修复；
- InnoDB：合并从 MySQL 5.6.44 到 5.7.26 的变化、修复程序 crash 等问题；
- Replication：修复 slave crash；
- CVE-2019-2614
- CVE-2019-2627
- CVE-2019-2805
- CVE-2019-2740
- CVE-2019-2739
- CVE-2019-2737
- CVE-2019-2758
- CVE-2020-2922
- CVE-2021-2007
- 在 MariaBackup、Read-only replicas、FULLTEXT INDEX、ALTER TABLE、System-Versioned Tables 等方面进行了 BUG 修复或程序改进
- CVE-2019-2974
- CVE-2019-2938
- CVE-2020-2780
- CVE-2021-2144
- 修复 InnoDB 当 FTS 表具有 FK 关系时启动失败的问题

- 在 General Server、Mariabackup、InnoDB、Aria、Optimizer、Replication、Security 等方面进行了 BUG 修复或功能改进，如修复内存对齐、死锁问题等
- Events：修复了从 Mariadb 10.3.19 中，禁用了由具有不同 server_id 的服务器创建的所有事件。请注意，该修复程序不会重新启用受影响的事件；
- CVE-2020-2752
- CVE-2020-2812
- CVE-2020-2814
- CVE-2020-2760
- CVE-2020-13249
- InnoDB、Replication、Optimizer 以及其他模块进行 BUG 修复或功能改进
- CVE-2021-2022。
- CVE-2020-15180。
- CVE-2020-14812
- CVE-2020-14765
- CVE-2020-14776
- CVE-2020-14789
- CVE-2020-28912
- CVE-2021-2194
- 修复查询优化器以 key_column [not]的形式处理构造（大量常数）时会消耗大量内存的问题；
- 涉及 PHP PDO、mysqlnd、mysql-connector-python 的问题修复。
- CVE-2021-27928

- CVE-2021-2166
- CVE-2021-2154
- CVE-2022-21451
- CVE-2021-2372
- CVE-2021-2389
- CVE-2021-46658
- CVE-2021-35604
- CVE-2021-46667
- CVE-2021-46662
- CVE-2022-27385
- CVE-2022-31624
- CVE-2022-24052
- CVE-2022-24051
- CVE-2022-24050
- CVE-2022-24048
- CVE-2021-46659
- CVE-2022-0778
- CVE-2022-21595
- 修复上一版本手动运行 mariadb-upgrade 时的阻塞问题；
- CVE-2021-46665
- CVE-2021-46664
- CVE-2021-46661
- CVE-2021-46668
- CVE-2021-46663
- CVE-2023-5157
- CVE-2018-25032
- CVE-2022-32091
- CVE-2022-32084

- CVE-2022-38791
- InnoDB:修复使用 SYSTEM VERSIONING 时的 Full-text index 问题；
- 修复序列引擎上的并行 slave 死锁问题；
- CVE-2022-47015

8.238. mate-desktop：

- 修复 valgrind 检查 kylin-control-center 有内存泄漏问题
- 修复软件包图形界面没有繁体中文问题
- 修复 multipath-tools-0.8.4-6.p04.ky10 卸载时报 mate-desktop 相关报错

8.239. mate-indicators：

- 修复在某些时区下，日历显示异常问题

8.240. mate-power-manager：

- 修复手动安装屏幕提示 error 信息

8.241. mate-session-manager：

- 修复注销后 mate-session 对自启动程序没有进行处理问题
- 修复错误的命令 gsettings set org.mate.session idle-delay -9999 执行成功不报错的问题

8.242. maven-surefire：

- 修复因 maven-shared-utils 升级导致的编译失败问题

8.243. mcelog：

- 修复 sysfs.c 文件 read_field 函数中 buf 变量长度未定义、使用完后未释放以及警告问题。

8.244. mdadm：

- 修复--monitor -r 的段错误
- 修复执行 mdmon md 生成 crash
- 修复 NULL ptr 引用和内存泄漏。
- 修复 mdadm:不打开用于 CREATE 和 ASSEMBLE 的 md 设备问题
- 修复 2 个流缓冲区错误。
- 修复 strcpy 的缓冲区大小警告。
- 修复 set_new_data_offset 中错误的“goto”
- 修复增长 RAID5 时的挂起问题
- super1：修复 1.0 元数据的 data_offset 设置。
- raid6check:修复 valgrind 检测到的内存泄漏
- Grow.c:修复未初始化的变量编译时错误
- 修复 super1.c 中位图偏移集的符号扩展

8.245. mesa：

- 修复内存泄露导致的花屏问题，

8.246. microcode_ctl：

- CVE-2022-40982：在某些英特尔处理器的某些矢量执行单元中瞬态执行后，通过微体系结构状态暴露信息可能允许经过身份验证的用户通过本地访问启用信息泄露。
- CVE-2022-38090：在使用英特尔® Software Guard Extensions 时，某些英特尔处理器中的共享资源隔离不当，可能会允许特权用户通过本地访问实现信息泄露。
- CVE-2022-33196：使用英特尔® Software Guard Extensions 时，某些英特尔® 至强®处理器的某些内存控制器配置中的默认权限不正确，这可能允许特权用户通过本地访问启用权限升级。
- CVE-2023-23583：处理器指令序列会导致某些英特尔®处理器出现意外行为，可能允许经过身份验证的用户通过本地访问实现权限升级和/或信息泄露和/或拒绝服务。

8.247. mobile-broadband-provider-info：

- 修复中文表述问题

8.248. mockito：

- 修复了 mockito 在 x86 架构上存在偶现的测试用例失败问题

8.249. mod_wsgi：

- CVE-2022-2255， 在 mod_wsgi 中发现了一个漏洞。X-Client-IP 标头不会从不受信任的代理的请求中删除，从而使攻击者能够将 X-Client-IP 标头传递给目标 WSGI 应用程序

8.250. mokutil：

- 修复了 delete_data_from_req_var 和 mok_get_variable 中删除数据内存泄漏的问题；
- 修复使用选项 cd:f:g::hi:lmpt:xDNPXv；
- 修复命令行参数显示问题

8.251. mtools：

- 修复解析配置文件不区分大小写问题。
- 修复调用 iconv 函数时的错误。
- 修复集群预分配中的错误
- 修复了 mcat 中图像末尾的错误行为。
- 修复 mformat 的 format_xdf 命令行参数
- 修复 mcopy 的问题

- 修复批处理模式下文件末尾的集群填充

8.252. mtr：

- 修复 mtr 无法发送 ipv6 的 udp 数据包的问题

8.253. multipath-tools：

- CVE-2022-41974，导致 multipathd 参数顺序修改以及 mpathpersist 命令执行失败的问题
- 修复 multipath -T 退出异常的问题
- 修复无效 remove 指令返回成功的问题

8.254. munge：

- 修复了 root 运行时检查失败的问题
- 修复了由 size_t ptr 强制转换引起的 big-endian 错误

8.255. mutt：

- CVE-2023-4874
- CVE-2023-4875
- CVE-2022-1328
- CVE-2020-14954

8.256. nagios：

- 解决使用命令“/usr/bin/cat /tmp/checkout2”。经过多次重新检查后，服务的输出将被截断；

8.257. nano：

- 修复 rc 文档空行上的越界读取

8.258. nasm：

- 修正 help info 的信息；
- CVE-2022-44370
- CVE-2020-21528

8.259. ncompress：

- 修复计算 maxmaxcode 时的整数溢出问题
- 解决 fd 泄露问题

8.260. ncurses：

- 修复 CVE-2023-29491

8.261. net-snmp：

- CVE-2022-24805，NET-SNMP-VACM-MIB 表设置中内存溢出问题

- CVE-2022-24806，修复输入验证
- CVE-2022-24807，修复内存溢出问题
- CVE-2022-24808，空指针解引用问题
- CVE-2022-24809
- CVE-2022-24810
- 修复 IF-MIB 相关多个问题
- CVE-2022-44792 ，修复 handle_ipDefaultTTL 中的空指针解引用导致程序崩溃的问题
- CVE-2022-44793，handle_ipv6IpForwarding 中的空指针解引用导致程序崩溃的问题
- 修复当加密 key 是 null 时创建用户异常问题

8.262. net-tools：

- 修复接口名称长度为 15 时 ifconfig 显示错误

8.263. NetworkManager：

- 修复 nftables：在 x86/arm/loongarch 架构下，默认防火墙管理工具为 iptables，NetworkManager 默认在此防火墙下进行网络管理，不支持 nftables 管理防火墙；
- 修复 pause 功能：在 x86/arm/loongarch 架构下，低版本不支持 nmcli 控制启动网卡 pause 模式功能；

- 修复混杂模式功能：在 x86/arm/loongarch 架构下，低版本不支持 nmcli 控制启动网卡混杂模式功能；
- 修复在港澳专版模式下安装操作系统，使用 nmtui 工具打开网络设置为英文版本，没有对应的繁体字版本支持；
- 修复 dbus 服务异常时 NetworkManager 服务无法自动启动；

8.264. nfs-utils：

- 修复 nfs_blkmapd 停止时的出现错误状态。
- 修复 systemd 读取 PID 文件失败问题。

8.265. nftables：

- 修复无效字段类型导致的崩溃
- 修复 parser_json 在解析设备时，在 netdev 家族源中不将字符串解析为 map 的判断的 bug.

8.266. nghttp2：

- CVE-2023-44487 ,HTTP/2 协议允许客户端通过发送 RST_STREAM 帧来指示服务器应该取消之前的流。该协议允许客户端单方面请求取消，这种攻击被称为快速重置
- CVE-2023-35945: HTTP/2 编解码器在从上游服务器接收到 GOAWAY 帧的 RST_STREAM 时可能泄露报头映射和记账结构

8.267. nginx：

- CVE-2022-41742：在模块 ngx_http_mp4_module 中存在漏洞，该问题可能允许本地攻击者导致工作进程崩溃，或者使用特制的音频或视频文件可能导致工作进程内存泄露；当 nginx 构建时启用 ngx_http_mp4_module，并在在配置文件中使用 mp4 指令时，攻击者可以使用特制音频或视频文件进行攻击。
- CVE-2022-41741：NGINX 在模块 ngx_http_mp4_module 中存在漏洞，可能允许本地攻击者破坏 NGINX worker 内存，使用特制的音频或视频文件导致其终止或潜在的其他影响。当 nginx 构建的时候启用 ngx_http_mp4_module，并在配置文件中使用 mp4 指令时，攻击者可以利用此模块的漏洞用特制音频或视频文件进行攻击。
- 修复 include 指令在 if 和 limit_except 块中不起作用的问题；
- 修复 ngx_http_xslt_filter_module 和 ngx_http_ssi_filter_module 等模块中的问题；
- CVE-2019-9511
- CVE-2019-9513
- CVE-2019-9516
- 修复使用 gzip 时可能在日志中出现 zero size buf 的警报，
- 修复在 SMTP 代理中使用 resolver 指令可能引发 worker 进程 segmentation
- 修复使用 HTTP/2 时 worker_shutdown_timeout 指令可能无法工作的问

题；

- 修复使用 HTTP/2 时 proxy_request_buffering 指令可能引发 worker 进程 segmentation 的问题；
- 修复读取客户端请求时使用 return 指令总是报错的问题；
- 修复请求 URI 末尾的转义字符不完整被忽略；
- 修复 URI 末尾的/.和/..不统一问题；
- 修复 merge_slashes 和 ignore_invalid_headers 指令中的问题；
- 修复 rewrite 指令在配置时使用空字符串可能引发段错误的问题；
- 修复 break 指令在与 alias 指令或者带 URI 的 proxy_pass 指令一同使用可能以引发段错误的问题
- 修复在 SSL 连接中处理 pipelined 请求可能超时的问题；
- 修复使用 HTTP/2 时 de 问题_points 指令中的问题；
- 修复 Transfer-Encoding 请求头被忽略的问题；
- 修复使用 HTTP/2 socket 泄漏问题；
- 修复使用 OSCP 工作进程可能段错误的问题；
- 修复 ngx_http_mp4_module 中的问题；
- 修复 error_page 指令产生的 494 错误码为 400；
- 修复在 njs 模块和 aio 指令中使用子请求发生 socket 泄漏的问题；
- 修复当使用 gRPC 后端工作时可能出现“upstream sent frame for closed stream”错误的问题；
- 修复 resolver 指令未指定时 OCSP 可能报错的问题；

- 修复使用不正确的 HTTP/2 preface 连接时未记录的问题
- 修复 SIGQUIT 期间没有删除删除 unix 域侦听套接字、没有代理长度为 0 的 UDP 数据包、使用 SSL 代理 uwsgi 后端可能不起作用等问题，
- 修复 ssl_ocsp 指令错误处理时的问题，
- 修复在 XFS 和 NFS 文件系统上磁盘缓存大小可能计算错误的问题，
- 修复 memcached 服务返回格式错误的响应可能引发“negative size buf in writer”
- 修复使用 ssl_ocsp 指令发生内存泄漏的问题
- 修复瞬时连接时可能产生“zero size buf in output”警告的问题、
- 修复在不同虚拟机上使用不同大小的 large_client_header_buffers 可能导致段错误的问题、
- 修复 SSL 关闭可能无法工作的问题、
- 修复 SSL_shutdown()接口失败的问题、
- 修复在 in the ngx_http_slice_module 和 ngx_http_xslt_filter_module 模块问题
- 修复当后端错误码为 500, 502,503, 504,403,404,或 429 时 stale-if-error 缓存控制扩展被错误应用的问题；
- 修复可能出现“cache file ... has too long heade”报错的问题；
- 修复 SSL_shutdown()接口失败的问题
- 修复延迟关闭时 SSL shutdown 不起作用的问题；
- 修复使用 gRPC 后端时可能出现“upstream sent frame for closed str

eam”错误的问题；

- 修复当 upstream 块中的 server 被标记为“down”时出现“no live upstr eams”错误的问题；
- 修复使用 HTTPS 时产生段错误的问题；
- 修复某些 HTTP 请求导致 400 错误以及 ngx_http_flv_module 和 ngx_ht tp_mp4_module 模块中的问题；
- 修复 return 指令与 image_filter 或 xslt_stylesheet 指令同时使用时 HE AD 请求处理不正确问题
- 修复 nginx 没有使用 ngx_mail_ssl_module 无法构建的问题；
- 修复使用 gRPC 后端可能产生“upstream sent response body larger than indicated content length”错误的问题；
- 修复客户端关闭了连接，但是由于 keepalive timeout 导致 nginx 可能不关闭连接的问题；
- 修复 nginx 当等待 auth_delay 或 limit_req delay 时客户端已经关闭连接但无法检测的问题；
- CVE-2021-23017
- 修复在日志中使用 SSL 变量可能为空的问题；
- 修复在接收到 GOAWAY 帧后 gRPC 后端连接可能没有关闭的问题；
- 修复使用 select、poll 或者/dev/poll 方法时 gRPC 后台 SSL 连接可能 ha ng 住的问题；
- 修复了使用分块传输编码时$content_length 变量中的问题；

- 修复使用 HTTP/2 和 aio_write 指令时请求可能会 hang 住的问题
- CVE-2021-23017
- 修复自动重定向过程中没有转移尾部斜线特殊字符的问题；
- 修复邮件代理模块中使用 SMTP 管道可能导致连接意外关闭的问题；
- 修复日志中 SSL 变量可能为空的问题
- 修复 URI 中未转移特殊字符的问题
- 修复在接收到 GOAWAY 帧后 gRPC 后端连接可能没有关闭的问题；
- 修复 SSL 握手后 stream 模块中的 SSL 连接可能 hang 住的问题；
- 修复使用 select、poll 或者/dev/poll 方法时 gRPC 后台 SSL 连接可能 hang 住的问题；
- 修复请求中不含 Content-Length 时使用 HTTP/2 客户端请求总是写到磁盘的问题
- 修复分块传输编码中$content_length variable 变量的问题；
- 修复使用 HTTP/2 和 aio_write 指令时请求可能 hang 住的问题
- 修复当不带 SSL 的 HTTP/2 下使用 sendfile 或 aio 指令可能会 hang 住的问题

8.268. nodejs：

- CVE-2022-43548-pre-1.patch，CVE-2022-43548-pre-2.patch，CVE-2022-43548.patch，在 Node.js 版本<14.21.1，<16.18.1，<18.12.1，<19.0.1 中存在操作系统命令注入漏洞，这是由于 IsAllowedHost

检查不足导致的，因为 IsIPAddress 在发出允许重绑定攻击的 DBS 请求之前没有正确检查 IP 地址是否无效，所以很容易被绕过；

- CVE-2023-0286，在 X.509 通用名称中存在与 X.400 地址处理相关的类型混淆漏洞。此漏洞可能允许攻击者将任意指针传递给 memcmp 调用，使他们能够读取内存内容或实施拒绝服务。
- CVE-2023-0215，BIO 链有时候没有被正确清理，调用者传递的 BIO 仍然保留指向先前释放的过滤器 BIO 的内部指针。如果调用者接着在 BIO 上调用 BIO_pop()，则会发生 use-after-free。这很可能导致崩溃。
- CVE-2022-4304，在 OpenSSL RSA 解密实现中存在一个基于定时的侧信道，它足以在 Bleichenbacher 式攻击中通过网络恢复明文。为了实现成功的解密，攻击者必须能够发送大量的尝试消息进行解密。
- CVE-2022-4450，调用者负责释放这些缓冲区。可以构造一个产生 0 字节有效负载数据的 PEM 文件。在这种情况下，PEM_read_bio_ex()将返回一个失败代码，但将用一个指向已经释放的缓冲区的指针填充 header 参数。如果调用者也释放这个缓冲区，那么将发生双释放。这很可能导致经济崩溃。这可能被攻击者利用，他们有能力提供恶意的 PEM 文件进行解析，以实现拒绝服务攻击。

8.269. nss：

- 修复导入 pkcs12 的问题

8.270. ntfs-3g：

- CVE-2022-40284：修改 libntfs-3g/runlist.c 文件，在解压运行列表时拒绝零大小的运行段，避免合并没有运行段的运行列表

8.271. ntp：

- CVE-2020-15025
- CVE-2023-26551
- CVE-2023-26552
- CVE-2023-26553
- CVE-2023-26554
- CVE-2023-26555

8.272. numactl：

- 修复了使用“--touch”选项时的崩溃问题；
- 修复使用偏移时的分段错误；

8.273. nvmetcli：

- 修复 Test_invalid_input 在 py3 失败问题；
- 修复保存报告名称时不正确问题；
- 修正 xrange 在 py3 的使用；

- 修正拼写错误；

8.274. opencc：

- 修复中文表述问题

8.275. openhpi：

- 解决安装后的服务自动重启失败问题

8.276. OpenIPMI：

- 修复执行 ipmi_ui -c smi test 时，直接 quit 会出现 coredump 的问题

8.277. open-iscsi：

- 修复 iscsid 守护进程 oom_score_adj 的设置不正确问题

8.278. openldap：

- CVE-2022-29155，解决 sql 注入问题
- CVE-2023-2953，解决空指针解引用问题

8.279. openmpi：

- 修改编译依赖 java-devel 改为 java-1.8.0-openjdk-devel 解决编译问题。

8.280. openpgm：

- 修复系统输出函数出现问题

8.281. openscap：

- 为 kyinos 新增 cpe 信息，以便进行扫描策略的选择,解决使用 scap-security-guide 中的安全基线选项运行结果报错的问题

8.282. opensc：

- CVE-2021-42780
- CVE-2021-42782
- CVE-2023-2977
- CVE-2023-40660
- CVE-2023-40661

8.283. openssh：

- 修复国密模式下 ssh 或 scp 连接新主机时国密算法类型显示错误。
- CVE-2023-38408，该漏洞仅涉及 openssh 提供的 ssh-agent 功能。当系统中使用了 ssh-agent 功能，此漏洞使攻击者能够控制服务器上的转发代理套接字，并能够写入客户端主机的文件系统，从而使用运行 ssh-agent 的用户的权限执行任意代码。
- 修复 ssh-agent 在添加动态库时的路径缺失问题

- CVE-2023-51385,在某些情况下，远程攻击者可能能够通过使用包含 shell 元字符的用户名或主机名的扩展令牌（例如 %u、%h）来执行任意操作系统命令。
- CVE-2023-48795，通过在握手期间操纵序列号，攻击者可以删除安全通道上的初始消息，而不会导致 MAC 故障。
- 修复 ssh 远程连接使用 kex 模式下存在内存泄露风险；

8.284. openssl：

- 修复空指针解引用导致内存分配错误
- 修复 evp_EncryptDecryptUpdate 中的整数溢出
- 修复静态代码分析工具 Coverity 中未初始化指针读取的问题
- 修复静态代码分析工具 Coverity 1498611 和 1498608 中未初始化读取的问题
- 修复静态代码分析工具 Coverity 1498607 中未初始化值的问题
- 修复 OBJ_nid2obj 总是引发错误的问题
- 修复 ssl_security_cert_chain 中的崩溃
- 修复 EC_GROUP_new_from_ecparam 中的未定义行为
- 修复 ec_key_simple_oct2priv 中的内存泄漏
- 修复 asn1_item_embed_new 中的崩溃
- 修复 CBC_MA 中缓存行为 32 字节时的泄漏
- 修复 crl_set_issuers 中的内存泄漏

- 修复 aarch64 静态链接报错的问题。
- 解决了 pkeyutl 的在原有版本上的验签失败的功能问题
- CVE-2023-5678
- CVE-2023-3817
- CVE-2023-3446
- CVE-2023-2650
- CVE-2023-0464，CVE-2023-0465，CVE-2023-0466
- CVE-2022-4450，CVE-2022-4304，CVE-2023-0215 and CVE-2023-0286
- CVE-2022-2097，CVE-2022-2068，CVE-2022-1292
- CVE-2023-5678,使 DH_check_pub_key 和 DH_generate_key 更安全

8.285. openvswitch：

- 修复 ofproto-dpif 模块中存在内存泄漏
- 修复 ovsdb-client 模块中存在内存泄漏
- 修复 ofproto 模块中 dpif_sflow_actions 函数中的拼写错误；
- 解决 datapath 模块 dpif_execute() 函数的 ofproto_mutex 锁递归问题；
- 解决数据路径的转换 xlate_table_action()函数在执行过程中遇到错误时没有正确地恢复之前的 table_id 的问题；
- 修复 ovs_key_ct_tuple_ipv 中传递给内核的数据初始化问题；
- 修复 dpif-netlink 模块中的流表项操作缺陷；
- 修复 dp_hash 和 recirc 动作不协调导致的数据包在 datapath 中无限循环并最终被丢弃的问题；

- 修复 Netlink 消息中包含过大的用户数据时的消息缓冲区溢出问题；
- 修复 ICMP 连接跟踪状态可能没有被正确地设置为 ICMPS_REPLY 的问题；
- 修复 decode_ed_prop() 函数重新分配 ofpbuf 的功能缺陷；
- CVE-2015-8011
- CVE-2020-27827
- CVE-2020-35498
- CVE-2022-4338
- CVE-2023-1668
- CVE-2023-5366

8.286. opusfile：

- CVE-2022-47021, opusfile.c 中的函数 op_get_data 和 op_open1 中发现了一个空指针取消引用问题
- 修复操作顺序允许中间值 pcm_total+diff 溢出 64 位 int 的范围溢出问题
- 修复左移运算左值类型问题

8.287. osinfo-db：

- 修复 cockpit 创建虚拟机产品化信息未被识别问题

8.288. pam：

- 可移植性修复，文档改进，翻译更新。
- pam_unix 修复了 CVE-2020-27780 -当用户不存在且 root 密码为空时绕过认证的问题

8.289. pango：

- 修复中文表述错误

8.290. pbzip2：

- 修复 pbunzip2、pbzcat 命令不可用

8.291. pcp：

- 修复了 pcp 提供的 dstat 命令格式化输出错误的问题。
- 解决中文系统环境下报错的问题
- 修复解析 IPI0 字段异常引起的 coredump 问题

8.292. pcre2：

- 修复启用无效 utf 时 ascii 单词类的无效匹配
- 修复记录数据多行匹配未命中问题
- 修复 JIT 中的递归问题
- 修复 JIT 中字符重复的回溯优化问题
- 修复条件争用问题

- CVE-2022-1586，unicode 属性匹配问题
- CVE-2022-1587，

8.293. perl-Carp_Clan：

- 修复错误 test 用例的 warning 提示

8.294. perl-Crypt-OpenSSL-Guess：

- 解决 OpenSSL 即使没有安装 Homebrew 也会显示可能的安装路径的问题

8.295. perl-Data-Dump：

- 修复字符串为“NaN”的类型仍转为 str 字符串问题

8.296. perl-Data-UUID：

- 通过减少引用次数修复内存泄漏，适当地使用 C 字符串

8.297. perl-Date-Manip：

- 修复 Date::Manip::Recur 函数输出错误问题
- 意大利语错误修复
- 修复 Date::Manip::Date::list_holidays 方法

8.298. perl-Encode：

- CVE-2021-36770，对 Perl5 进程的当前目录具有写访问权从而进行命令执行

8.299. perl-ExtUtils-CBuilder：

- 修复了 Base.pm 正则表达式

8.300. perl-File-Listing：

- 修复到 2038 年日期溢出问题

8.301. perl-Getopt-Long：

- 修复了一个 bug:当一个选项有:s%设置且未传入任何参数时，会导致 Perl 警告，现在改为显示实际的错误消息

8.302. perl-HTML-Parser：

- 修复 eof 上的堆栈混淆错误：在 eof 解析后，Parser.xs 无法调用 SPAGAIN 的问题

8.303. perl-HTTP-Cookies：

- 修复没有处理 HttpOnlycookie 的主机名前面加上的#HttpOnly_,HTTP:：

Cookies:：Netscape 的问题

- 修复在请求头中通过设置 max-age 值来规定缓存策略时未按预期处理的问题

8.304. perl-HTTP-Message：

- 解决 HTTP::Request 中 uri_canonical 崩溃的问题
- 修复在 MSWin32 上使用 Use File::Spec 失败问题；
- 修复 HTTP::Request::Common 简介中的示例

8.305. perl-HTTP-Tiny：

- CVE-2023-31486，更新默认 TLS 配置，默认情况下开启 ssl 校验功能

8.306. perl-libwww-perl：

- 更新持久化文件修改时间失败时输出警告信息，备份临时文件的处理修复
- 修复 redirect.t 用例中的一些小概率失败问题

8.307. perl-LWP-Protocol-https：

- 修正 copyright 年限

8.308. perl-MRO-Compat：

- 修复 prototypes 方法

8.309. perl-Net-LibIDN2：

- 修复未使用变量的编译警告

8.310. perl-Pod-Coverage：

- 修复安装路径冲突问题，'/usr/share/perl5/vendor_perl/Pod' /usr/share/perl5/vendor_perl/Pod 不是该包独有的路径，是多个 perl 安装包共用的路径

8.311. perl-Pod-Parser：

- 修复安装路径冲突问题，'/usr/share/perl5/vendor_perl/Pod' /usr/share/perl5/vendor_perl/Pod 不是该包独有的路径，是多个 perl 安装包共用的路径

8.312. perl-Pod-Perldoc：

- 修复安装路径冲突问题，'/usr/share/perl5/vendor_perl/Pod' /usr/share/perl5/vendor_perl/Pod 不是该包独有的路径，是多个 perl 安装包共用的路径

8.313. perl-Sub-Name：

- 解决符号"DPPP_my_croak_xs_usage"未定义问题

8.314. perl：

- CVE-2023-31484
- CVE-2023-31486

8.315. pesign：

- CVE-2022-3560
- 修复工具验证文件发生“bad note description”错误的问题
- 修复证书链错误

8.316. php：

- 解决文件系统加载程序在加载名称为用户输入的模板时遇到问题；
- 解决 phar 解压缩程序代码会递归地解压缩 quines gzip 文件将导致的无限循环的问题
- 修复缓冲区移除导致的加密属性被消除问题
- 修复 PDO::quote()中未捕获的整数溢出
- 修复 HTTP 表单上传中的部分数量过多导致的服务拒绝问题
- 修复客户端向服务器泄露 31 位未初始化的内存、恶意服务器更容易猜测客户端的随机数的问题；
- 修复 PHP 可访问的任何本地文件被泄露问题；
- 修复加载 phar 文件时堆栈缓冲区溢出问题；

- 修复核心路径解析函数分配的缓冲区太小导致的未经授权的数据访问或修改问题；
- 修复当 password_verify()函数接受一些无效的 Blowfish 哈希作为有效哈希导致的允许此条目的任何密码有效的问题

8.317. pinfo：

- 解决 filehandling_functions 中当间接信息节点丢失时不会显示错误信息的问题
- 解决 video.c 中当 regexp 匹配到空字符串时会无限循环的问题
- 修复当访问未打开过的文件时会出现段错误的问题
- 修复 ncurses autoconf 测试中的链接顺序出现错乱的问题

8.318. pixman：

- CVE-2022-44638，修复由于 pixman_sample_floor_y 中的整数溢出，rasterize_edges_8 中存在越界写入问题

8.319. pkgconf：

- CVE-2023-24056：由于 libpkgconf/tuple.c 文件中函数 pkgconf_tuple_parse 里的不正确检查，变量重复可能导致无限字符串扩展，造成缓冲区的溢出。

8.320. pluma：

- 修复显示行号覆盖显示的问题

8.321. pmix：

- CVE-2023-41915

8.322. polkit：

- CVE-2021-4115，允许非特权用户通过进程文件描述符用尽导致 polkit 崩溃

8.323. poppler：

- CVE-2022-27337，修复 Hints::Hints 函数中存在一个逻辑错误，这使得攻击者能够通过构造特定的 PDF 文件来发动拒绝服务（DoS）攻击；
- CVE-2022-37050，PDFDoc::savePageAs 函数允许攻击者通过构造一个 PDF 文件来引发拒绝服务攻击
- CVE-2022-37051，pdfunite.cc 中的主要函数在保存嵌入文件之前缺少流检查，导致了一个可达的终止错误，进而引发拒绝服务攻击
- CVE-2022-37052，一个可达的 Object::getString 断言因 markObject 的失败，使得攻击者能够引发拒绝服务攻击
- CVE-2022-38349，在 Object.h 中存在一个可达的断言，这会导致拒绝服务攻击，因为 PDFDoc.cc 中的 PDFDoc::replacePageDict 函数在保存嵌

入文件之前缺少流检查

- CVE-2020-23804，在 poppler 0.89.0 版本的 pdfinfo 和 pdftops 中，存在未受控制的递归问题
- CVE-2020-36023， 该漏洞源于使用精心设计的 PDF 文件通过 FoFiType1C::cvtGlyph 方法可以造成拒绝服务攻击；

8.324. popt：

- 修复对 poptStuffArgs 遗存的不当处理避免内存泄露

8.325. postfix：

- 修复 postfix 包安装存在空链接文件问题

8.326. postgresql-jdbc：

- CVE-2022-41946， 如果输入流大于 2k，则使用 PreparedStatement.setText（int，InputStream） 或 PreparedStatemet.setBytea（int，InputStream）的预处理语句将创建一个临时文件，同一系统上的其他用户可读取它们

8.327. postgresql：

- CVE-2021-20229，这个缺陷允许对一列具有选择权限的用户创建一个特殊查询，返回表的所有列。这个漏洞的最大威胁是保密性。

- CVE-2021-32028，在 postgresql 中发现一个缺陷。使用 INSERT ... ON CONFLICT...在一个专门制作的表上执行 UPDATE 命令，经过身份验证的数据库用户可以读取服务器内存的任意字节。该漏洞的最大威胁是数据的机密性。

8.328. ppp：

- CVE2022-4603. pppdump/pppdump.c 文件的函数 dumpppp 存在漏洞，参数 spkt.buf/rpkt.buf 的操作可能会导致数组索引的验证不正确
- 修复了 ppp 两端配置为只发送另一方的 IP 地址而不发送自己的 IP 地址时的特殊场景下的问题

8.329. procps-ng：

- CVE-2023-4016

8.330. proftpd：

- 修复构建--localstatedir 配置选项的使用
- 修复了使用 TLSv1.3 上传大文件的 FTPS 问题
- 修复了 From 指令中 IPv6 地址的处理
- 修复了目录列表延迟中的回归
- 修复了数据传输过程中的释放后使用漏洞
- 通过删除捆绑的 libcap，并仅依靠系统提供的 libcap，解决了 mod_cap

中读取的越界问题。当 libcap 库可用时，从源代码构建 ProFTPD 才会自动包含 mod_cap 模块

- CVE-2019-18217 -修复了预认证远程拒绝服务问题
- CVE-2021-46854，1.3.7c 之前的 proftpd 中的 mode_radius 允许 RADIUS 服务器泄露内存，因为它复制了 16 个字符的块

8.331. protobuf-c：

- CVE-2022-33070
- 解决了 parse_required_member 函数无符号整形溢出问题。

8.332. protobuf：

- CVE-2021-22570，当空字符出现在 proto 信号中时，Nullptr 指针会被取消引用。proto 信号解析错误，导致在生成错误信息时未选中对 proto 文件名的调用。由于 proto 信号解析错误，文件显示为 nullptr。

8.333. pulseaudio：

- 解决 从 gnome 图形界面启动时，pulseaudio 下的 gsettings-helper 出现 coredump 问题

8.334. pyflakes：

- 修复类作用域中未定义的 qualname 名称

- 修复某些类型构造中的假阳性（TypeVar、NamedTuple、TypedDict、cast）
- 修复与其他装饰器和非全局作用域中的 @overload 检测
- 修复对异步函数的 @overload 检测

8.335. python2：

- CVE-2019-20907，Lib/tarfile.py 文件存在输入验证错误漏洞，该漏洞源于_proc_pax 缺少标头验证

8.336. python3：

- CVE-2021-4189
- CVE-2022-0391
- CVE-2015-20107
- CVE-2021-28861
- CVE-2020-10735
- CVE-2022-37454
- CVE-2023-24329

8.337. python-attrs：

- 增加了 @attr.s(collect_by_mro=False) 参数。如果设置为 True，则可以修复从基类收集属性。
- 修复了 ValueError：Cell is empty 错误，该错误可能发生在一些罕见的

边缘情况中。

- 修复了当默认值无法直接与 == 进行比较时（例如 numpy 数组）的 auto_attribs 的使用方式。
- 修复了存根文件，以防止 mypy 的 disallow_any_generics=True 选项引发的错误。
- 修复了当 slots=True 被设置时原始类在被替换后仍保持活动状态的引用泄漏问题。

8.338. python-blivet：

- 添加使用 xfs_repair 检查和修复 XFS 的支持
- bug 修复：
- 修复磁盘安装的部分中文翻译
- 修复安装期间 brtfs 上的删除子卷错误
- 修复了 test_action_dependencies 中 LV 最小大小的调整
- 修复了在 action_test 中检查文件系统支持的问题
- 修复分区的可调整大小属性
- 修复从 sysfs 读取模型时可能出现的 UnicodeDecodeError
- 修复 DM 完整性格式的状态
- 修复 MD 设备及其分区的名称解析(vtrefny)
- 修复读取隐藏的 sysfs 属性
- 修复了忽略父或子磁盘设备的问题

- 拼写错误修复
- 修复了 srpm 和 rpm Makefile 目标中的源 tarball 清理问题
- 修复了在 collect_mbrs 中试图关闭 fd 时出现的 UnboundLocalError 错误
- 让 parted 修复分区表的可修复问题
- 修复了忽略隐藏设备的日志信息
- 修复了 Anaconda 的“suggestion _container_name”
- 修复 LVM VDO 设备的外部依赖
- 修复 LVM VDO 逻辑卷的类型
- 修复了在 SELinuxContextTestCas 中设置 SELinux 标志的问题
- 修复从缓存中获取 LVMPhysicalVolume 中的 PV 信息的问题
- pylint:修复 get_cow_sysfs_path 中的异常字符串
- pylint:修复异常中多个未使用的变量'e'
- flags:修复泄漏文件描述符
- 修复了在 libblockdev 2.23 及更早版本下检查 LVM VDO 支持的问题
- 修复 ActionRemoveMember 要求检查
- 修复了名称看起来像 BIOS 驱动器号的解析设备
- 修复/统一在测试中导入模拟模块
- 修复激活旧式 LVM 快照的问题
- 修复了在 lvm_test 中使用 assert_called_with 的问题
- 修复 udev 中过多的日志

- 修复了翻译中的 pylint 错误
- 修复读取 sysfs 属性时可能出现的 UnicodeDecodeError
- 修复运行 BlivetLVMVDODependenciesTest 测试用例为非根

8.339. python-bottle：

- 修复一些模块__file__为空的问题

8.340. python-certifi：

- CVE-2022-23491：Certifi 2017.11.05 到 2022.12.07 版本存在数据伪造问题漏洞，攻击者利用该漏洞可以从根存储的“TrustCor”中删除根证书。
- CVE-2023-37920：Certifi 2023.07.22 之前版本存在数据伪造问题漏洞，该漏洞源于 e-Tugra 的根证书存在安全漏洞。

8.341. python-cryptography：

- CVE-2023-23931：ciphers.py 文件中，_CipherContext 类的 update_into 方法将接受实现缓冲区协议的 Python 对象，但只提供不可变的缓冲区。这将允许不可变对象（如 bytes）被变异，从而违反 Python 的基本规则，导致输出损坏。
- 解决在 backend.py 文件中没有证书的情况下加载 pkcs#7 数据结构时产生的程序崩溃问题。
- 解决在 backend.py 文件中当加载 pkcs#7 数据结构失败时仅返回一个空

列表而不抛出异常的问题。

8.342. python-dasbus：

- 修复一个 DBus 调用超时抛异常的 BUG

8.343. python-execnet：

- 解决远程状态检测错误问题

8.344. python-httplib2：

- CVE-2021-21240

8.345. python-hypothesis：

- 修复了一个错误，即我们的示例数据库逻辑无法区分基于@pytest.mark.parameize（...）参数的失败示例。
- 修复了一些我们以前可能无法运行某些策略的验证逻辑的情况。

8.346. python-importlib-metadata：

- 解决问题，在 PyPy2 与 PyPy3 修复 repr(EntryPoint)
- 解决问题，修复项目元数据，正确声明 python_requires 指令
- 解决问题，修复 PyOxider finder 没有__module_属性的问题
- 解决问题，修复 FastPath.zip_children 中的冗余条目

8.347. python-joblib：

- CVE-2022-21797：由于 eval（）语句，1.2.0 之前的 joblib 容易受到通过 Parallel（）类中的 pre_dispatch 标志执行任意代码的影响

8.348. python-jwt：

- 修正 is_pem_format 的参数作物

8.349. python-lxml：

- CVE-2022-2309，解决 libxml2 无法在解析器上下文中重置名称空间计数错误问题

8.350. python-marshmallow：

- 修复了在 AwareDateTime 中键入的问题。
- 修复了在未指定键或值 Field 时让 Dict 在反序列化时传递无效 dict 的 bug。
- 修复了 unknown=INCLUDE 时虚线键的处理方式
- 修复了在实例化具有名为 parent 的字段的架构时引发 AttributeError 的 bug。
- 修复字段。TimeDelta 序列化精度。
- 修复 Schema.validate 中数据参数的类型提示，以接受字典列表。

- 解决 Python 3.10 中的 distutils 弃用警告。
- 修复在 Field._serialize 签名中输入的问题。
- 修复嵌套部分架构的默认继承。
- 修复调用 get_declared_fields：再次传递 dict_cls。

8.351. python-more-itertools：

- 修复 python 3.7 导入某些类型的弃用警告。

8.352. python-paramiko：

- CVE-2022-24302
- 修复 OpenSSH 密钥格式下支持 ECDSA 密钥的 BUG

8.353. python-pbr：

- 修复 python3-pbr 安装时需要 python2 的问题

8.354. python-pexpect：

- 修正了超时后截断 before 属性的错误；

8.355. python-pillow：

- CVE-2022-22815、CVE-2022-22816 的现象一致：在 9.0.0 版本之前的 Pillow 中，path.c 中的 path_getbbox 在 ImagePath.Path 初始化期间存

在缓冲区过度读取。

- CVE-2022-45198：低于 9.2.0 的 Pillow 对高度压缩的 GIF 数据执行不当处理（数据放大），导致缓冲区溢出
- CVE-2023-44271， 它会不受控制地分配内存来处理给定的任务，可能会因内存不足而导致服务崩溃。
- CVE-2022-45199， Pillow 允许通过 SAMPLESPERPIXEL 拒绝服务
- CVE-2022-24303， Pillow 是一个 PIL(Python 成像库)分支。受此包影响的版本容易受到输入验证不当的影响。当 Linux 或 macOS 上的临时目录路径包含一个空格时，这将破坏 im.show()(和相关操作)之后删除临时图像文件的操作，并可能删除一个不相关的文件。
- CVE-2021-23437， 在 getrbg 函数中，可以构造 Regular Expression Denial of Service（正则表达式拒绝服务）攻击。

8.356. python-pip：

- CVE-2020-14422，Lib/ipaddress.py 文件的 IPv4Interface 和 IPv6Interface 存在资源管理错误漏洞，该漏洞源于程序未正确计算哈希值
- CVE-2021-33503，Urllib3 存在资源管理错误漏洞，该漏洞源于在鉴权模块的 URL 中添加@参数导致

8.357. python-psutil：

- 修复 Linux 的磁盘 I/O 计数器失败的问题

8.358. python-pyasn1：

- 修复了如何验证分配给构造类型的项目设计错误；

8.359. python-pygments：

- 解决 get_tokens_unprocessed 中的无限循环问题

8.360. python-reportlab：

- CVE-2023-33733，绕过 rl_safe_eval 利用 HTML 标签的 Color 属性远程执行代码，该属性的内容被直接认为是使用函数的 python 表达式，从而导致代码执行。
- CVE-2020-28463， 这个漏洞通过 img 标签进行服务器端请求伪造（SSRF），可以利用服务器的功能来发送恶意请求，从而访问或控制内部资源。

8.361. python-requests：

- CVE-2023-32681，当通过 HTTPS 发送时，Proxy-Authorization 头必须作为 CONNECT 请求发送，因为代理无法查看隧道中的请求。这导致 Requests 无意中将代理凭据转发给目标服务器，使恶意行为者可能泄露敏感信息。

8.362. python-setuptools：

- CVE-2022-40897,由于 package_index.py 中存在一个正则表达式拒绝服务（ReDoS）的问题，漏洞可使用一个定制的包或 PackageIndex 页面中插入 HTML 来造成拒绝服务攻击

8.363. python-simplejson：

- 修复 python-simplejson 卸载不完全，遗留文件夹没删除干净，导致 flask 使用时报错的问题

8.364. python-slip：

- 修复 sender_seen 中的内存泄露问题

8.365. python-tornado：

- CVE-2023-28370

8.366. python-urllib3：

- 修改 RECENT_DATE 为当前时间，修复由于时间问题导致的编译问题。
- 修复了端口“0”返回“无”的问题。
- 修复将导致错误的字段 NRESERVED_PAT 和函数_idna_encode。
- CVE-2023-43804。
- CVE-2023-45803。

8.367. python-werkzeug：

- CVE-2023-23934
- CVE-2023-25577

8.368. qemu：

- 修复上游代码中 SSBS 字段错误问题
- 新增龙芯架构的支持，解决龙芯架构编译问题
- CVE-2023-2861
- CVE-2023-0664
- CVE-2023-3180
- CVE-2023-3354
- CVE-2020-24165
- CVE-2020-13791
- CVE-2021-3638
- CVE-2022-35414
- CVE-2021-3507
- CVE-2021-20257
- CVE-2020-13253
- CVE-2021-3607
- CVE-2021-3608
- CVE2022-0216
- CVE-2022-4144
- CVE-2022-1050
- 解决龙芯架构启动虚拟机时 bootorder 顺序不起作用

- 修复使用 virtio-gpu 优化问题
- 修复 qemu 标准输出重定向无数据

8.369. qpid-proton：

- 修复 python3 动态库支持问题，

8.370. qt5-qtbase：

- CVE-2023-24607，当使用 SQL ODBC 驱动程序插件并且 SQLTCHAR 的大小为 4 时，6.4.3 之前的 Qt 允许通过特制的字符串拒绝服务。
- CVE-2023-32762 和 CVE-2023-32763，Qt 网络错误地解析了严格传输安全（HSTS）标头，允许建立未加密的连接，即使服务器明确禁止也是如此。如果用于此标头的大小写不完全匹配，则会发生这种情况；渲染包含图像的 SVG 文件时，可以触发 QTextLayout 缓冲区溢出。
- CVE-2023-37369，QXmlStreamReader 中可能会通过精心设计的 XML 字符串导致应用程序崩溃，从而触发前缀为大于长度。
- CVE-2023-33285，QDnsLookup 有一个缓冲区过读，通过一个来自 DNS 服务器的精心设计的回复；根据描述，此 CVE 影响 Qt5.x 和 Qt6，对 Qt 4 不影响。
- CVE-2023-34410，TLS 的证书验证并不总是考虑链的根是否是已配置的 CA 证书。
- CVE-2023-38197，在递归实体展开中存在无限循环。

- CVE-2023-43114，当使用 GDI 字体引擎时,如果通过 QFontDatabase::addApplicationFont{FromData]加载损坏的字体，因为缺少长度检查，那么它可能会导致应用程序崩溃。

8.371. qt5-qtsvg：

- CVE-2021-45930，修复在调用QPainterPath::addPath and QPathClipper::intersect 两个方法时会出现 QtPrivate::QCommonArrayOpsQPainterPath::Element::growAppend 两个方法越界写入

8.372. qt5-qtwebengine：

- 修复在内核 64K 页的情况下，Qt5-QtWebEngine 运行的程序段错误问题

8.373. qt：

- CVE-2023-32573，QtSvg QSvgFont m_unitsPerEm 初始化处理不当。
- CVE-2023-34410，TLS 的证书验证并不总是考虑链的根是否是已配置的 CA 证书。
- CVE-2023-38197，在递归实体展开中存在无限循环。
- CVE-2023-37369，QXmlStreamReader 中的应用程序可能会因为一个精心制作的 XML 字符串而崩溃，该字符串会触发前缀大于长度的情况。
- CVE-2023-43114，当使用 GDI 字体引擎时,如果通过 QFontDatabase::addApplicationFont{FromData]加载损坏的字体，因为缺少长度检查，

那么它可能会导致应用程序崩溃。

- CVE-2023-32573
- CVE-2020-0570
- CVE-2020-17507

8.374. quota：

- 修复 systemd 读取 quota_nld 生成的 PID 文件概率性失败的问题。
- 修复 XFS 配额的宽限期溢出。
- 修复 XFS 文件系统上的限制设置。
- 修复忽略禁用配额的问题
- warnquota：注解 CC_TO 是通过 LDAP 解决的，
- warnquota：修复帮助文本

8.375. radvd：

- 修复：多次给 radvd 发生 sighup 信号，会导致 radvd 服务异常出现内存泄露问题

8.376. rasdaemon：

- 修复不完整的磁盘错误日志。
- 修复可能但不太可能的文件描述符泄漏。
- 修复 RAS-MC-CTL.SERVICE 在 selinux 开启时启动失败的问题。

- 修复 unistd.h 读写函数的返回值类型问题。

8.377. rdma-core：

- 修复扩展 sge 内存空间时没有内存对齐的问题。

8.378. re2：

- 修复 64 位转 32 位的 clang 警告。

8.379. realmd：

- 修复 realmd 加入 2016 AD 服务器时，产生的问题
- 修复带有“realm join”的 AD DC 的 IP 地址作为参数添加到“ad_server”选项 inssd.conf 中产生的问题。
- 使用 PKG_PROG_PKG_CONFIG 修复交叉编译

8.380. redis：

- 修复 HyperLogLog 在基本情况下处理错误偏移量的问题。
- 修复 HyperLogLog 的损坏问题。
- 修复 redis-check-aof 中潜在的溢出问题。
- 修复键空间通知类别不匹配的问题。
- 修复 genericZrangebylexCommand 中的 zlexrangespec 内存泄漏。
- 修复了 AOF 实现中的重要问题。

- CVE-2021-32626,
- CVE-2021-29478
- CVE-2021-32672
- CVE-2022-36021
- CVE-2023-28856

8.381. resource-agents：

- 修复从 pid-file 文件获取 pid 失败的问题

8.382. rest：

- 修复调用 rest_xml_parser_parse_from_data 时，如果传递参数为空字符串会导致 crash 的问题

8.383. rhash：

- 修复从标准输入读取 file-list 的问题

8.384. rpmdevtools：

- 修复 rpmdev-checksig、rpmdev-rmdevelrpms -l 命令执行之后报 TypeError 异常问题

8.385. rpm：

- CVE-2021-35937，本地非特权用户可以利用这个缺陷绕过响应 CVE-2017-7500 和 CVE-2017-7501 时引入的检查，从而可能获得根权限
- CVE-2021-35939，该漏洞源于没有对中间目录执行不安全符号链接检查。攻击者利用该漏洞可能会获取到 root 权限
- CVE-2021-35938，该漏洞源于当 rpm 在安装文件后设置所需的权限和凭据时，就会出现符号链接问题。
- 解决了在 fork 出来的运行小脚本的进程的信息补阻塞的问题。
- 修复事务终止 scriptlets 期间 ctrl-c 上的倒退
- 同步了上游多个补丁解决各种内存问题和其它问题。

8.386. rsync：

- CVE-2022-29154
- CVE-2022-37434

8.387. rsyslog：

- CVE-2022-24903

8.388. rubygem-nokogiri：

- CVE-2022-24836

8.389. ruby：

- CVE-2023-36617

- CVE-2023-28755
- CVE-2023-28756
- CVE-2021-33621

8.390. samba：

- 修复 libsmbconf 和 libsamba-errors 库文件的版本号，libsmbconf 变化 0->0.0.1，libsamba-errors 变化 1->1.0.0。
- 调整 KDB 模块中的 sign_authdata 以适用于 krb5 v1.18，从而修复 samba 服务重启失败的问题。
- CVE-2022-32743，Samba 未验证 dNSHostName 属性的 Validated-DNS-Host-Name 权限，这可能会允许无权限用户写入该属性。
- CVE-2022-3437，在 Heimdal 的 GSSAPI unwrap_des()和 unwrap-des3()例程中的 Samba 中发现了一个基于堆的缓冲区溢出漏洞
- CVE-2022-42898，1.19.4 之前的 MIT Kerberos 5（又名 krb5）和 1.20.1 之前的 1.20.x 中的 PAC 解析存在整数溢出，在 32 位平台上可能导致远程代码执行（在 KDC、kadmind 或 GSS 或 Kerberos 应用程序服务器中）（导致基于堆的缓冲区溢出），并在其他平台上导致拒绝服务。
- CVE-2022-44640，由于密钥分发中心（KDC）使用的 ASN.1 编解码器中存在无效自由，因此 7.7.1 之前的 Heimdal 允许远程攻击者执行任意代码。
- CVE-2022-45141，由于微软已于 2022 年 11 月 8 日披露了 Windows Kerberos RC4-HMAC 权限提升漏洞，并且根据 RFC8429 假设 rc

4-hmac 很弱，因此尽管目标服务器支持更好的加密（例如 aes256-cts-hmac-sha1-96），但存在漏洞的 Samba Active Directory DC 仍会发出 rc4-hmac 加密票据。

- CVE-2022-38023，Netlogon RPC 权限提升漏洞。
- CVE-2023-0922，Samba AD DC 管理工具在远程 LDAP 服务器上运行时，默认情况下将通过只签名连接发送新密码或重置密码。
- CVE-2022-2127，由于 winbindd_pam_auth_crap.c 中的长度检查不足，在 Samba 中发现越界读取漏洞。
- CVE-2023-34966,在用于 Spotlight 的 Samba mdssvc RPC 务中发现无限循环漏洞。
- CVE-2023-34967， 在用于 Spotlight 的 Samba mdssvc RPC 服务中发现了类型混乱漏洞。
- CVE-2023-4091， 漏洞允许 SMB 客户端截断文件，即使在 Samba VFS 模块 "acl_xattr "配置为 "acl_xattr:ignore system acls = yes" 时具有只读权限。SMB 协议允许在客户端请求只读访问时打开文件，但如果客户端指定了单独的 OVERWRITE 创建处置请求，则会隐式地将打开的文件截断为 0 字节。该问题出现在绕过内核文件系统权限检查、完全依赖 Samba 权限的配置中。
- CVE-2023-42669，该漏洞源于一个可无限期阻塞的 RPC 函数。出现这个问题的原因是，"rpcecho "服务的主 RPC 任务中只有一个 Worker，这就允许对 "rpcecho"服务器的调用在指定时间内被阻塞，从而导致服务中

断。在特定条件下，"dcesrv_echo_TestSleep() "函数中的 "sleep()"调用会触发服务中断。已通过身份验证的用户或攻击者可利用此漏洞调用 "rpcecho"服务器，要求它在指定时间内阻塞，从而有效地中断大多数服务，并导致 AD DC 完全拒绝服务。由于 "rpcecho "在主 RPC 任务中运行，因此 DoS 会影响所有其他服务。

8.391. sblim-sfcb：

- 修复 cim 软件包提供的 schema 文件默认位置和 sfcb 软件包不对应问题

8.392. scap-workbench：

- 将规则标题和描述字体颜色设置为黑色，修复诊断窗口中显示的错误

8.393. screen：

- CVE-2023-24626,如果 screen 有 setuid 或者 setgid 的权限，那么普通用户可以通过 screen 发送 SIGHUP 信号给任意进程，让进程挂起

8.394. SDL2：

- CVE-2022-4743，

8.395. sed：

- 修复临时文件清理，代码有时会在调用 fclose（FP）后使用 FP,这在 C 中

具有未定义的行为

8.396. sendmail：

- 添加 procmail 安装依赖，修复发送邮件时缺少 procmail 命令。
- 修复执行 newaliases 命令报错
- 修复 postfix 功能异常；

8.397. sg3_utils：

- 修复 rescan-scsi-bus.sh 语法错误
- 修复’m LEN’ < 252 导致的 coredump 问题

8.398. shadow：

- CVE-2013-4235，O_NOFOLLOW 是 Linux 系统下 open 系统调用的一个标志位，用于在打开文件时防止符号链接（symlink）攻击。当设置了 O_NOFOLLOW 标志时，open 将不会跟随符号链接打开文件
- CVE-2023-4641，相关内存清零、防止密码泄露
- CVE-2023-29383， 释放 libsemanage 的内部资源，在删除用户时也释放密钥
- 修复 userdel 的内存泄漏（valgrind）释放已移除的数据库条目

8.399. shim：

- 支持更多的硬件设备和修复了一些启动问题
- CVE-2023-0286
- CVE-2017-3735
- CVE-2017-3737
- CVE-2018-0732
- CVE-2018-0739
- CVE-2019-1563
- CVE-2020-1971
- CVE-2021-23841
- CVE-2022-0778
- CVE-2021-3712

8.400. sip：

- 解决子包打包文件冲突问题

8.401. sleuthkit：

- 修复 fuzz 测试 hfs_cat_traverse()和 hfs_dir_open_meta_cb()出现的越界读取问题。
- 修复 tsk/base/tsk_base_i.h 中的左移运算错误
- 修复 ntfs 中的 memleak

8.402. snakeyaml：

- CVE-2022-41854：那些使用 Snakeyaml 解析不受信任的 YAML 文件

的人可能容易受到拒绝服务攻击

- CVE-2022-25857：由于缺少集合的嵌套深度限制，0 和 1.31 之前的包 org.yaml:snakeyaml 容易受到拒绝服务 (DoS) 攻击。
- CVE-2022-38749、CVE-2022-38750、CVE-2022-38751、CVE-2022-38752：使用 snakeYAML 解析不受信任的 YAML 文件可能容易受到拒绝服务攻击(DOS)。如果解析器在用户提供的输入上运行，攻击者可能会提供导致解析器因 stackoverflow 而崩溃的内容。

8.403. snappy-java：

- CVE-2023-34454，Snappy.java 中存在未经检查的乘法，导致有可能出现整数溢出，从而引发不可恢复的致命错误。
- CVE-2023-34455，SnappyInputStream.java 中存在未经检查的块长度，当长度异常将导致不可恢复的致命错误。
- CVE-2023-43642，SnappyInputStream 在解压缩块大小过大的数据时容易受到拒绝服务（DoS） 攻击。

8.404. sox：

- CVE-2021-33844
- CVE-2023-32627
- CVE-2021-23159
- CVE-2023-34432
- CVE-2023-34318

- CVE-2021-23172
- CVE-2021-3643
- CVE-2021-23210
- CVE-2022-31650
- CVE-2023-26590
- CVE-2022-31651
- CVE-2023-32627
- CVE-2017-18189

8.405. sqlite-jdbc：

- CVE-2023-32697

8.406. squashfs-tools：

- 修复 unsquashfs“write outside directory”漏洞。
- 修复 unsquashfs 写入程序线程中的错误处理。
- 修复在中止追加时截断目标的故障。

8.407. squid：

- CVE-2021-46784，由于缓冲区管理不当，在处理较长的 Gopher 服务器响应时可能会发生拒绝服务。
- CVE-2022-41317， 使用代理的客户端通过 HTTPS 请求到内部缓存管理器 URL 时，可能会暴露敏感信息
- CVE-2022-41318，libntlmauth 发现缓冲区超读。由于不正确的整数溢出

保护，SSPI 和 SMB 身份验证帮助程序容易读取非预期的内存位置。在某些配置中，这些位置的明文凭据会被发送到客户端。

- CVE-2023-46846，squid 存在 HTTP 请求走私漏洞，该漏洞由分块解码器宽松性引起，允许远程攻击者通过防火墙和前端安全系统执行请求/响应走私。
- CVE-2023-46847，Squid 存在拒绝服务漏洞，当 Squid 配置为接受 HTTP 摘要验证时，远程攻击者可通过向堆内存写入多达 2 MB 的任意数据来执行缓冲区溢出攻击。
- CVE-2023-46724，由于存在指定索引验证不当漏洞，使用 `--with-openssl`编译的 Squid 3.3.0.1 至 5.9 以及 6.4 之前的 6.0 版本易受针对 SSL 证书验证的拒绝服务攻击。
- CVE-2023-46728， Squid 容易受到针对 Squid 的 Gopher 网关的拒绝服务攻击。
- CVE-2023-49285，由于存在缓冲区超读漏洞，Squid 容易受到针对 Squid HTTP 消息处理的拒绝服务攻击
- CVE-2023-49286， 由于函数返回值检查错误，Squid 容易受到针对其辅助进程管理的拒绝服务攻击
- CVE-2023-50269， 存在不受控制的递归错误，Squid 可能会受到针对 HTTP 请求解析的拒绝服务攻击。当配置了 follow_x_forwarded_for 功能时，该问题允许远程客户端通过发送大的 X-Forwarded-For 头来执行拒绝服务攻击。

8.408. sssd：

- 修复 sssctl/sssctl_domains.c 中的空指针解引用问题
- 修复 sssd_be 进程的 coredump 问题

8.409. strongswan：

- CVE-2022-40617，证书指向的服务器在初始 TCP 握手后什么都不做，或者发送过多的应用程序数据，从而在吊销插件中造成拒绝服务

8.410. sudo：

- CVE-2023-42465，1.9.15 之前的 Sudo 可能允许 row hammer 攻击（用于身份验证绕过或权限提升）
- CVE-2022-37434，zlib 1.2.12 版本存在安全漏洞，该漏洞源于在 inflate.c 中通过一个大的 gzip 标头额外字段在 inflate 中具有基于堆的缓冲区过度读取或缓冲区溢出
- CVE-2022-33070，protobuf-c/protobuf-c.c 中的函数 parse_tag_and_wiretype 包含无效的算术移位
- CVE-2022-43995，plugins/sudoers/auth/passwd.c 数组越界错误，
- 修复某些 message 的大小导致校验和错误的问题
- 修复 sudo_passwd_verify 函数内涉及到密码存放的内存没有清零的问题
- 修复在 role_to_sudoers 函数中存在 use-after-free 的问题

- 修复内存汇漏的问题，在 plugins/sudoers/auth/pam.c 文件中的 converse 函数中存在内存泄漏，pass 指针里没有 free
- CVE-2023-22809，当用户指定的编辑器包含绕过 sudoers 策略的“–”参数时，拥有 sudoedit 访问权限的本地攻击者可通过将任意条目附加到要处理的文件列表中，最终在目标系统上实现权限提升
- CVE-2023-28486，在 1.9.13 版本之前不会转义日志消息中的控制字符
- CVE-2023-28487，Sudo 无法转义 sudoreplay 输出中的控制字符
- 修复/etc/sudo.conf 和/etc/dnf/protected.d/sudo.conf 两个文件在更新包时存在覆盖问题

8.411. supermin：

- 修复 ext2 复制内核模块错误的问题
- 修复无法在 hce 上检测到包管理器的问题

8.412. sysfsutils：

- 修复 sysfs_device.c 和 sysfs_attr.c 两个文件中的内存泄漏问题

8.413. syslinux：

- 解决主包和 perl 包中的 syslinux2ansi.1.gz 文件重复问题。

8.414. sysstat：

- CVE-2022-39377：allocate_structures 在 sa_common.c 中包含 size_t 溢出。allocate_structures 函数未充分检查边界，导致表示系统活动的缓冲区溢出。
- CVE-2023-33204：sysstat 到 12.7.2 允许 check_overflow 中的乘法整数溢出。
- 修复使用 iostat 命令确定 DM 设备是否是新创建时计算结果可能溢出的问题。
- 修复使用 mpstat 命令 iowait 瞬高的问题。

8.415. systemd：

- 修复 systemd 重命名网卡设备会有旧设备残留问题
- 修复更正 linux 下正确的引用头文件
- 修复在 switch-root 情况下 mount 和 unmount 不能正确的序列化问题
- 修复网络在初始化 loop 回环的问题
- 修复 sd-device 结构体中 usec_initialized 的类型正确问题
- 修复 CVE-2022-3821,会导致 format_timespan()中的缓冲区溢出，从而导致拒绝服务
- 修复 CVE-2023-26604，权限管理不当漏洞；
- 修复 asan 内存地址检查测试所报告的的堆栈溢出问题
- 修复 growfs 重新设置大小 resize 的问题
- 修复目录 fd 的问题

- 修复创建临时文件和目录的问题
- 修复 coredump 崩溃时 stdout 和 stderr 输出的问题
- 修复 cgroup agent 的 stdout 和 stderr 输出显示问题
- 修复 mdns 包匹配过滤问题
- 修复潜在的缓冲区溢出修复一个错误
- 修复日志试图重复关闭 fd 问题
- 修复进程 1 的并发共享 nss 查找问题
- 修复通过 D-Bus 获取属性 OnExternalPower 的问题
- 修复查询状态导致的段错误和异常触发 SIGNAL 等等问题
- 修复配置解析中行号问题
- 修复 jobs 残留的问题、服务启动顺序异常的问题、配置文件字段不生效问题
- 解决执行特定的服务 systemctl start testC.target，执行 systemctl reload testA.service，testA、testB、testC 的启动顺序异常的问题
- 解决设置/etc/systemd/system.conf 文件中 StatusUnitFormat=name 后，不生效的问题
- 解决 pstore 中的 use after free 内存错误
- 解决 udevadm 中缺少描述符初始化的问题
- 修正 udev 错误修正函数的内存泄露
- 修复 network ndisc 中 prefixes 清除不彻底的问题
- 修复 nspawn 中对--console=help 的处理错误

- 修正 sd-device 模块 enumerator 部分设备移除时不应该返回错误码的问题
- 修正 chown 和 chmod 设备节点文件时的返回码、忽略 ENOENT
- 修正设备文件 perm 属性修改时的日志的错误码、忽略 ENOENT
- 修正 systemd-analyze verify 命令运行时的 seg fault
- 修正 core path 模块中对前一个状态的同步问题
- 修正 udevd manager 结束后 monitor 继续运行的问题
- 修复 bernate-resume-generator 无限等待唤醒设备的问题
- 修复 hibernate-resume-generator 中的 generator name 信息错误
- 修复 udevadm trigger 发生 coredump 问题；
- 修复 busctl 执行超时打印错误日志；
- 修复 systemctl 的打印信息过早结束问题；
- 修复 journal 日志打印次数不对问题；
- 修复 TTYPath=参数和标准输出/输入一起使用验证报错；
- 修复 mount 添加 make-rprivate 属性没有生效的问题
- 修复服务使用 KillMode=mixed 后 ExecStopPost 进程存在残留的问题；
- 修复在存在大量块设备的情况下首次使用普通用户 ssh 远程登录系统卡顿问题；
- 修复 loongarch 外置光驱按按钮后无法正常弹出问题；

8.416. tang：

- CVE-2023-1672,服务器的竞争条件漏洞，它影响了密钥生成和密钥旋转的功能。这个漏洞导致了一个很小的时间窗口，使得 Tang 私钥可以被同一主机上的其他进程读取。

8.417. tar：

- CVE-2023-39804,漏洞源于 PAX 存档中的扩展属性处理不当，允许远程攻击者在目标系统上执行任意代码

8.418. tboot：

- 更新 LCP-GEN2 工具（wxWidgets 通配符错误修正）
- 修复由扩大的 tb_hash_t 联合引起的堆栈溢出。
- 修复“避免不安全功能”扫描后的警告。
- tools:修复 klocwork 报告的一些 dereference-NULL 问题。

8.419. tcl：

- 修复 CVE-2021-35331，nmakehelp.c 中的格式字符串漏洞可能允许通过精心制作的文件执行代码，形成注入型攻击等

8.420. tcpdump：

- CVE-2023-1801，tcpdump 中的 SMB 协议解码器在解码制作的网络数据包时执行越界写入的问题

8.421. texlive-base：

- 修复 texlive-base 部分二进制文件和 so 存在 rpath 风险
- CVE-2023-32700，1.17.0 之前的 LuaTeX 允许编译一个不受信任的 tex 文件时执行任意 shell 脚本
- 修复 texlive-lib 存在空链接文件的问题

8.422. thin-provisioning-tools：

- 修复读取无效子树根时可能出现的内存错误

8.423. tigervnc：

- CVE-2023-1393

8.424. tomcat：

- 解决未能拒绝无效标头的请求、可能导致的请求走私攻击问题
- 解决用户代理能够通过不安全的通道传输会话 cookie 问题
- 修复安装后存在三个软连接文件指向的目标文件为空的问题
- 修复表单身份验证功能中，打开重定向情况下，URL 存在重定向到不受信任站点的问题
- 修复将单个请求视为多个请求、从而导致在反向代理之后进行请求走私的问题

8.425. tpm2-abrmd：

- 修复指针指向无效地址的问题

8.426. tpm2-tss：

- CVE-2023-22745，layer_handler 数组，之前的大小定义为 255，但实际上允许的值是 0-255，所以数组需要调整大小为 256.缓冲区溢出可能导致任意代码执行

8.427. traceroute：

- 修复 Linux 内核版本大于等于 6.1 的无特权 ICMP tracerouting 问题
- CVE-2023-46316。

8.428. transfig：

- 修复将一个 fig 图像转化为 png 图片，报告 ghostscript 不可见问题

8.429. tuned：

- 修复了父代包含共同祖先的多重继承问题；
- scheduler 针对 sched_*和 numa_*调优参数进行了接口抽象，以解决 5.13 及更新内核下将一些 sched_* 和 numa_*参数从 sysctl 移动到 debug fs 的问题；

- net 类别下修复了各种回溯问题；
- cpu-partitioning 配置修复了在较新内核上 no_balance_cores 问题；
- 调优 profile 文件中修复了对 include 指令的不正确解析；
- tuned-gui 修复 profile 文件保存和注释等问题
- 修复了 tuned 2.18 版本中内联注释的解析问题；

8.430. tzdata：

- 更新 java source 版本为 1.8，对应修改编译命令，解决编译问题。

8.431. uboot-tools：

- CVE-2022-30767：squashfs 文件系统实现包含一个基于堆的缓冲区溢出漏洞，这是由于元数据读取过程中的缺陷造成的。
- CVE-2022-34835：do_i2c_md 的组件:i2c md Command Handler 中的整数符号错误和缓冲区溢出会导致 do_i2c_md 函数的返回地址指针损坏（手动调试的不合法输入可导致 内存损坏）。

8.432. udisks2：

- 修正软件包的 license
- 解决停止 udisks2 进程时出现的 daemon_resource 实例被重复释放问题。

8.433. ukui-greeter：

- 修复登录失败锁定 1 分钟显示为英文问题；
- 修复 mips 架构，用户密码锁定后登录界面仍存在锁定用户问题；
- 修复某些情况下登录界面的密码框无隐藏图标-小眼睛
- 修复系统注销后会在登录界面弹出应用客户端窗口
- 修复 passwd 锁定用户密码之后，登录界面仍显示锁定的用户；
- 修复登录系统输入密码框右边的眼睛提示在锁屏切换用户注销的策略不一致；
- 修复使用 kylin 管理员用户登录，登录界面 kylin 用户名字显示不全；
- 修复相同 uid 用户锁屏时没有头像；
- 修复多个普通用户 uid 相同，控制面板和登录界面显示错误；

8.434. ukui-screensaver：

- 修复相同 uid 用户锁屏无头像的问题；
- 修复锁屏背景图片全部删除后，锁屏界面背景异常；
- 修复 vnc 会话结束后有锁屏程序的异常进程问题；
- 修复系统锁屏后，环境中若是有弹窗，会有焦点占用的问题；
- 修复繁体翻译问题；

8.435. unbound：

- CVE-2022-3204
- CVE-2022-30698

- CVE-2022-30699
- 修复 -q 与“unbound-control stats_shm”命令一起使用时应该不工作问题；

8.436. undertow：

- CVE-2023-1108，由于在 SslConduit 中更新了意外的握手状态，这个问题使得拒绝服务成为可能，因为循环永远不会终止，进程将进入死循环

8.437. vdo：

- 修复了 vdo 用户空间工具中的缓冲区溢出问题;
- 修复了 vdoby_dev 工具中的一个问题,该问题可能导致当 vdo 配置文件中的某些设备不存在时，启动 vdo 设备。

8.438. vim：

- CVE-2023-2609
- CVE-2023-2610
- CVE-2023-2426
- CVE-2023-1264
- CVE-2023-1170
- CVE-2023-1175
- CVE-2023-0433
- CVE-2022-47024
- CVE-2023-0288

- CVE-2023-0049
- CVE-2023-0051
- CVE-2023-0054
- CVE-2022-4292
- CVE-2022-4293
- CVE-2022-3491
- CVE-2022-3520
- CVE-2022-3591
- CVE-2022-4141
- CVE-2022-3705
- CVE-2022-3324
- CVE-2022-3297
- CVE-2022-3296
- CVE-2022-3352

8.439. virglrenderer：

- CVE-2022-0135
- CVE-2022-0175

8.440. virt-manager：

- 新增龙芯架构支持，主要是支持安装虚拟机、以及解决安装过程中不显示网络设备的问题；
- 解决 uefi 启动的虚拟机不支持 bochs 视频显示的问题
- 解决 virt-install 使用默认的 1G 内存安装虚拟机失败的问题
- 解决 cockpit 调用 virt-install 创建虚拟机，点击重启后未成功的问题

8.441. watchdog：

- 修复%preun 和% postn 中的 watchdog.ping.service 为 watchdog-ping.service；
- 修复潜在的缓冲区溢出；
- 将无内存错误视为不可修复的错误：当内存不足时，重新启动机器；

8.442. wayland：

- CVE-2021-3782；修复内部引用计数保存在缓冲池中，每次从池中创建新缓冲区时都会递增，造成内存泄漏；

8.443. webkit2gtk3：

- CVE-2023-28204，在处理恶意网络内容时，可能会出现越界读取，从而导致信息泄露

8.444. wireshark：

- 解决系统语言为繁体时，开始菜单 wireshark 应用程序名称显示为英文的问题

8.445. xfsdump：

- 修复 FTBFS 错误。

- 修复可能导致备份损坏的绑定挂载场景

8.446. xfsprogs：

- 修复使用容量特别小的磁盘或镜像文件使用了 stripe geometry 进行创建后再进行 mkfs.xfs 格式化操作，mkfs.xfs 会报 ASSERT 问题。
- 修改 xfs_agf_verify()对 agf 的 freeblocks 进行校验，如果校验失败就返回，这个可以解决某些条件下 sync 卡住问题；
- 修正__xfs_dir3_free_read()返回值进行修改，不返回空指针；
- 修正 xfs_dabuf_map()在分配失败的时候返回 ENOMEM；
- 修正 xfs_alloc_ag_vextent_lastblock()修正对 len 的使用，应使用指针；
- 修复 xfs_db 中 crc 失效导致的段错误；
- 修正缺失的目录缓冲区损坏检查；
- 修正 inode 分配块 res 计算优先级；
- 修复 inode 分配块保留计算中的“偏移一位”错误；
- 修复 xfs_attr_shortform_verify 中的边界错误；
- 修正 xfs_defer_agfl_block()设置 xefi_skip_discard；
- 修复 nlink 值打印问题；
- 修复删除事务时 inode 预留大小不对问题；
- 修正 dir3_sf_entry_flds[]里使用 E3OFF 而不是 EOFF。。

8.447. xkeyboard-config：

- 修复中文描述错误

8.448. xorg-x11-server：

- CVE-2022-2319，由于请求长度验证不当，ProcXkbSetGeometry 函数中可能会出现越界访问问题。
- CVE-2022-2320，ProcXkbSetDeviceInfo 请求时存在特定缺陷。该问题是由于缺乏对用户提供的数据的正确验证导致的，这可能导致内存访问超出分配的缓冲区的末尾。此漏洞允许攻击者提升权限并在 root 上下文中执行任意代码。
- CVE-2022-3551，ProcXkbGetKbdByName 函数在遇到错误时不会释放分配的数据，从而导致内存泄漏。
- CVE-2022-3553， xquartz 的文件 hw/xquartz/X11Controller.m 的未知部分。操纵导致拒绝服务。
- CVE-2022-4283，XkbCopyNames 函数留下了指向已释放内存的悬垂指针，导致后续 XkbGetKbdByName 请求的内存访问越界。
- CVE-2022-46340，XTestFakeInput 请求发送长度大于 32 字节的 GenericEvents，XTest 扩展的 XTestFakeInput 请求的交换处理程序可能会破坏堆栈。
- CVE-2022-46341，XIPassiveUngrab 请求的处理程序在使用高键码或按钮代码调用时访问越界内存

- CVE-2022-46342， XvdiSelectVideoNotify 请求的处理程序可能会在内存被释放后写入内存。此问题可能导致 X 所在系统上的本地权限提升。
- CVE-2022-46343， ScreenSaverSetAttributes 请求的处理程序可能会在内存被释放后写入内存。此问题可能会导致 X 服务器运行特权的系统上的本地权限提升以及 ssh X 转发会话的远程代码执行。
- CVE-2022-46344， XIChangeProperty 请求的处理程序存在长度验证问题，从而导致越界内存读取和潜在的信息泄露。此问题可能会导致 X 服务器运行特权的系统上的本地权限提升以及 ssh X 转发会话的远程代码执行。
- 修复 openEuler hardcode 问题
- CVE-2023-0494，由于 DeepCopyPointerClasses 中的一个悬空指针引起的，ProcXkbSetDeviceInfo（）和 ProcXkbGetDeviceInfo（（）可以利用该指针读取和写入释放的内存。这可能会导致 X 服务器为 ssh-X 转发会话运行特权和远程代码执行的系统上的本地权限提升。
- CVE-2023-1393，在 X.Org 服务器覆盖窗口中发现一个缺陷。免费后使用可能导致本地权限升级。如果客户端显式破坏合成器覆盖窗口（也称为 COW），Xserver 会在 CompScreen 结构中留下一个指向该窗口的悬空指针，这将在稍后释放后触发使用。
- CVE-2022-3550，在 X.org 服务器中发现一个被归类为关键的漏洞。受此漏洞影响的是文件 xkb/xkb.c 的函数_GetCountedString。该操作导致缓冲区溢出。

- CVE-2023-5367， 在 xorg-x11-服务器中发现了一个越界写入缺陷。此问题是由于在复制存储在堆中的 Xi/xiproperty.c 中的 XIChangeDeviceProperty 函数和 randr/rrproperty.c 中的 RRChangeOutputProperty 函数中的数据时，缓冲区偏移量计算不正确，从而可能导致特权升级或拒绝服务。
- CVE-2023-5380， 在 xorg-x11-server 中发现释放后使用的缺陷。如果指针从一个屏幕上的一个窗口内扭曲到另一个屏幕的根窗口，并且原始窗口被破坏，然后另一个窗口被摧毁，那么 X 服务器可能崩溃。
- CVE-2023-6478， 巧尽心思构建的对 RRChangeProviderProperty 或 RRChangeOutputProperty 的请求可能会触发整数溢出，从而导致敏感信息泄漏。
- CVE-2023-6377，查询或更改 XKB 按钮操作（例如从触摸板移动到鼠标）可能会导致内存读写越界。在涉及 X11 转发的情况下，这可能允许本地权限提升或可能的远程代码执行。

8.449. xvidcore：

- 修复由于括号错误而导致的错误回归

8.450. yajl：

- CVE-2022-24795

8.451. yasm：

- CVE-2023-37732，在/libyasm/intnum.c 和/elf/elf.c 中有对空指针解引用

8.452. yhkylin-backup-tools：

- 修复/usr/bin/backup-daemon 这个进程在 dbus 处理 com.kylin.backup.manager.ghostbackup 参数过滤不严可以实现普通用户的提权操作问题

8.453. yp-tools：

- 修复整改 yp-tools 存在不安全函数 RAND_priv_bytes

8.454. zlib：

- CVE-2023-45853，MiniZip 在 zipOpenNewFileInZip4_64 中通过长文件名、注释或额外字段导致整数溢出和基于堆的缓冲区溢出
- CVE-2022-37434,
- CVE-2018-25032

8.455. zookeeper：

- 修复 Zookeeper 服务进行 reload 时的错误

8.456. zziplib：

- CVE-2020-18770：修改 mmappend.c，通过预先检查头部和尾部的标记，避免潜在的 ASAN:SIGSEGV 无效内存访问。

8.457. box-utils：

- 修复 KVE-2023-1202，低权限的攻击者可以通过 boxmount mount /etc 目录，进而修改/etc/passwd 文件，实现权限提升。

8.458. kysec-daemon：

- 修复三员用户家目录删除后,stirct 模式仍然可以成功切换,但无法登录的问题

8.459. kysec-utils：

- 修复三员用户家目录删除后,stirct 模式仍然可以成功切换,但无法登录的问题

8.460. box-manager：

- 开始菜单软件包名添加繁体中文
- 修复 box-manager 繁体翻译不全的问题

8.461. hsdimm-lite：

- 去掉 config.h.in~编译文件任务
- 兼容不同版本安全内存内核模块

8.462. kysec-common：

- 获取当前时间并转化为字符串，调用后需释放内存
- 日志接口设置超时时间
- 更新日志信息通讯传输方式
- 增加 sqlite stmt 类接口封装
- 从目录获取文件列表时返回绝对路径
- 修改 spec 文件,安装时重启服务
- 兼容 hostos 与 procps 调用
- 处理 kysec_log.h 中宏 gettid 冲突
- 增加 hostos 调用 procps 容错
- 修改解压 xz 文件的方式,提高解析文件类型的速度,修改 spec 文件，添加 xz 依赖
- 修复解析文件类型时,对没加!/bin/bash 头且文件后缀为.sh 的脚本文件判断不准确的问题，导致 source 执行文件时会把脚本文件当成普通文件放行

8.463. kysec-daemon：

- kmod_list 表初始化放在单独文件中，方便升级安装时还原数据；修改 sp

ec 文件，修改数据库重新初始化脚本

- 移除 libkysec 依赖，修改 spec 文件，删除编译依赖和安装依赖
- 统一 sqlite stmt 接口调用
- kysec-init 功能优化：系统安装好后首次启动进行 kysec 初始化期间，可以点击开始菜单进行关机重启，导致下次开机仍然要初始化修改 netctl 接口参数类型
- 修复数据库操作时句柄泄露问题
- 修复数据库锁定导致标记回退问题
- fortify 扫描漏洞修改
- 系统未启用 KYSEC 时，不进行初始化
- 解决添加换行符后全盘打标记的问题
- 解决数据库显示模块名称乱码的问题
- 强制模式下，提供 bash 执行脚本时哈希校验功能
- 解决通过 kysec_whlist_load 导致 kysec-daemon 进程终止的问题
- 更新文件保护标记时，同步更新 readonly_list 文件
- 新增安全套件状态配置
- 修复多次添加相同设备策略时，log 有 failed 信息问题
- 修复 koji 编包的问题
- 设备管控需求合入通用
- 嵌入式 E2000 设置 StorageDrive(当为启动盘时)开启状态，显示屏黑屏
- 内核模块化，未实现 exectl.ko 模块化，但是修改同样适用

- 适配主线及 hostos
- 配 hostos 内核 lsm 参数
- kysec 配置-进程保护标签设置-kysec_get 无法查看当前标记
- 切换模式时忽略 devctl 的状态值设置
- 卸载套件时清除策略
- 修复 hub 禁用启用不即时生效的问题
- 修复 security-switch --set strict 设置三元密码时，dbus 通信超时导致密码设置失败的问题
- 修复 strict 模式下，kysec-wlinit 失败的问题
- 同步桌面流量管控普通用户可以配置策略问题
- 修复 sm 套件取消授权失败的问题
- 修复 sm 查询文件保护错误的问题
- 修复切换模式时,会删除/etc/default/grub 中关于静态度量的配置
- 去掉切换 none 模式时 audit=0 的配置

8.464. kysec-sync-daemon：

- 核外更新数据库时，比较哈希值是否相同，不相同时才修改状态为已篡改状态
- kysoft 标记或 parent 标记的程序在 mv 只读标记的文件后，readonly 标记丢失，内核没有通知核外程序
- kysoft 标记或 parent 标记的程序在 mv 只读标记的文件后，readonly 标

记丢失，内核没有通知核外程序

- kysec 服务监听指定改为 127.0.0.1
- 优化系统启动服务；spec 文件中移除 kysec-sync.service
- 设备管控需求合入
- 兼容模式添加内核模块化补丁
- 修改 kmod 策略同步

8.465. kysec-utils：

- 进程防杀死：将/usr/sbin/activation-daemon 程序从进程防杀死列表移除，并添加到进程防杀死黑名单中去，解决开机时会出现 kylin-activation coredump
- 解决 rsync 增量备份功能失效的问题
- 修改 kysec 各模块状态时产生操作日志
- 规范化 dbus 接口返回值
- 修复释放 glib iter 崩溃问题
- 修复 kysec_monitor 的编译警告，修复 kysec_set 批量设置文件标记错误的问题，优化 getstatus 状态获取接口
- 修复联网管控 dbus 接口调用失败
- 内核通讯改用 tid 通讯；且重新实现 gettid 方法，修复 loongarch64 下 gettid 导致编译失败问题
- 修改 netctl 接口容错问题；添加装包时 netctl_pkg.xml 的同步功能

- kysec_get_process_info.c 的漏洞修复
- 修复 parent 标记进程在/var/lib/dpkg 目录下创建的文件无权限执行的 bug
- 修复 fortify 扫描的 bug
- 新增安全套件状态配置
- 优化判断 netlink 的方式；优化 netlink 通讯效率
- :修复关机过程调用 initramfs 内进程无执行权限的问题
- 修复 koji 编包的问题
- 修复 utils 与 common gettid 重名问题
- 修复 kysec_set 设置 netctl 提示信息有无误的问题
- 清空 netctl 默认黑名单配置文件
- 修复更新内核模块防卸载时没有 return 返回值
- 修改 spec 文件，取消对 libkysecwhlist-devel 编译依赖
- 解决 setstatus 设置 kysec enforcing 时卡住的问题
- setstatus 设置 kysec 为 enforcing 时，忽略 devctl，sm 和 pblk 的状态值设置
- 修复 kysec 关闭的情况下，设置 netctl 黑名单报错的问题
- 修复 hub 禁用启用不即时生效的问题
- 解决通过 sh 或者 python 执行 unknown 标记的文件,会产生两条重复的错误提示
- 解决在安装 tuned 包后，提示/etc/profile.d/env.sh 没有权限的问题

- 为 docker 容器运行的程序加上 kysoft 标记
- kysec 为 permissive 模式，且 exectl 为 enable 模式时，kysec_exectl_check()加入日志
- 同步桌面流量管控普通用户可以配置策略问题
- 修复切换 selinux 策略失败时，提示语句不完整的问题
- load_policy 和 checkpolicy 加入 secadm_list 文件中
- 修复 getstatus 在 sm 开启时未显示部分功能状态的问题
- 【外设管控】去除虚拟机默认策略中有 test 相关内容
- 修复三员用户家目录删除后,stirct 模式仍然可以成功切换,但无法登录的问题
- 修复查询或设置非模块文件的防卸载策略时，提示段错误
- 修复使用 source 执行普通文件是 kysec 拦截的问题
- 修复进程管控使用命令工具查询或者设置由 sdk 导致的错误
- 修复 sm 添加进程防杀死的失败的问题
- 修复 sm 查询文件保护错误的问题

8.466. security-switch：

- 修复 secadm 输错三次密码后仍可以切换状态的问题
- 修改使 securit-switch 切换状态后重启生效
- 修复安全模式切换失败时，存在多余输出信息的问题

8.467. libsecurity1：

- 解决通过 kysec_conf_set dbus 方法导致 kysec-daemon 进程终止的问题
- 修改 spec 文件，当升级安装时，不改变 kysec.conf 的配置
- kysec.conf 文件添加 kysec_pblk=0

8.468. libchkuid：

- 解决添加用户段错误的问题

8.469. security-reinforce：

- 修复普通用户使用 security-reinforce -f 命令会在终端一直卡住问题
- 修复执行 security-reinforce 命令-模板功能-导入/导出模板后按 ctrl+D 进入死循环“请输入导入文件路径 >该模板文件不存在”
- 修复 strict 模式下修改 bashrc 文件后，重启登录 secadm 用户提终端示权限不够
- 若相关文件在/目录下，修复关闭系统信任机制和删除潜在危险文件加固失败
- 修复麒麟安全模板默认加固项显示与设计文档不一致
- 修复加固和还原“设置登录后系统提示信息”后，没有执行重启 sshd 服务操作
- 修复 eu-objdump 组件包含在 elfutils 包中，检查可调试组件未对该包进

行检查

- 修复 eu-readelf 组件包含在 elfutils 包中，检查可调试组件未对该包进行检查
- 修复 aplay 组件包含在 alsa-utils 包中,检查可调试组件未对该包进行检查
- 修复 arecord 组件包含在 alsa-utils 包中，检查可调试组件未对该包进行检查
- 修复 readelf 组件包含在 binutils 包中，检查可调试组件时未对该包检查
- 修复交互命令删除不存在模板是没有提示信息
- 修复交互命令选择不存在模板编号时没有提示信息
- 修复选择不存在模板编号后再选择导入模板，终端高刷路径不存在信息
- 修复导出的安全报告格式没有对齐，显示不美观
- 修复非交互命令界面加固结果中“加固时间”应修改为“加固开始时间”
- 修复未进行加固扫描导出报告，出现的提示信息重复了 2 次
- 修复交互命令删除不存在模板是没有提示信息
- 修复 UI 界面和命令行导出的安全报告显示不一致，建议统一
- 修复“禁止 SSH 自动登录”的功能和加固名称
- 建议对同个加固项仅提供仅扫描和扫描并加固中的一种模式
- 加固项“禁用 printer 服务”应修改为“禁用 cups 服务”
- 【交互命令】导入、删除模板成功时建议给出提示
- 修复【非交互命令】自定义参数导入测试-关闭系统不必要的端口为 1 个端口时。安全加固失败，再次加固程序崩溃

- 修复设计文档中，“删除与设备运行、维护等工作无关的账号”加固项未归属在麒麟安全模板中
- 修复模板中“禁用 cups 服务”加固项的英文描述需要修改，将“printer”修改为“cups”
- 修复【潜在威胁】不存在 vnStatsvg 软件包，无法正确判断加固项状态
- 修复加固重要文件，加固报告中存在“etc/shadow”，应为绝对路径
- 修复安全加固界面创建的模板通过命令行导出后，无法再使用命令行导
- eu-objdump 组件包含在 elfutils 包中，检查可调试组件未对该包进行检查
- eu-readelf 组件包含在 elfutils 包中，检查可调试组件未对该包进行检查
- 建议删除 sync/shutdown/halt 账户
- 修复【安全加固】开启三元后，secadm 用户导出加固模板至 root 目录，提示“该路径不存在”
- 修复 strict 模式下，root 用户/审计用户执行扫描加固时，提示“普通用户没有加固权限”
- 修复安全用户导出模板至/root 目录，提示“导出目录路径不存在”
- 修复安全服务 motd 文件信息不符合要求时，ssh 成功登录后 Banner 项仍为无需加固
- 修复【安全服务】设置 ssh 登录前警告信息不符合要求时，扫描结果依然为无需加固
- 修复【安全服务】加固后，telnet 登录后警告信息语法错误
- 修复【安全服务】设置 telnet 登录前警告信息满足条件仍被加固，且信息

添加方式为追加

- 修复"设置 telnet 登录前警告 Banner"加固成功后没有生成 issue.net 文件
- 修复【系统审计】auditd 服务 disable 后，开启审计机制加固项扫描结果为无需加固
- 修复/etc/motd 内容为空，默认模板中“设置 telnet 登录后警告 Banner”后执行扫描，没有扫描出风险
- 修复模板中“禁止 SSH 免密登录”加固项标识需要修改
- 修复“禁止 SSH 免密登录”加固项分类错误
- 修复【非交互命令】导入模板 导入的文件为 Log 文件，服务崩溃
- 修复【系统设置】禁止系统自动登录为待加固状态，扫描结果依然为无需加固
- 修复“删除除 root 之外 UID 为 0 的用户”加固项名称与加固项功能不一致
- 修复【安全服务】禁用 ident 服务和禁用 bootps 服务，实际实现与加固项名称不一致
- 修复禁用不必要的系统服务和 xinetd 服务加固小项前，需加上大项分类名称
- 修复加固项“限制 FTP 用户上传的文件所具有的权限”在未安装 vsftpd 包的情况下提示“需手动加固”
- 修复【系统功能】三权模式下/etc/mail/aliases 和/etc/aliases 禁用不必要的别名，两次加固还原，第二次还原失败
- 修复【潜在威胁】还原后删除潜在危险文件，再次扫描还原失败

- 修复【潜在威胁】安全报告中检查可调试组件扫描结果缺少组件名称
- 修复【密码强度】仅删除/etc/pam.d/system-auth 文件中的参数，“加强口令的密码算法”加固项的扫描结果为“待加固”
- 修复【交互命令】输入导入路径时无法退出该界面
- 修复【非交互命令】未使用过安全加固时，-o 参数导出安全报告没有提示信息
- 修复密码复杂度设置更严格时，扫描结果依然为待加固
- 修复 system-auth 和 login.defs 文件中 sha512 配置均被注释后，“加强口令密码算法”扫描结果为无需加固
- 修复限制/boot/efi/EFI/kylin/grub.cfg 文件权限加固项名称与详情描述不符合规范
- 修复设置守护进程的 umask 值为 0777，依然会被加固
- 修复“禁止/var/log 日志文件全局可写”加固后文件权限为 640,建议调整为 644
- 修复【系统设置】“禁用 ctrl+alt+del 组合键”加固后状态为加固成功，实际 tty 界面重启生效
- 修复【潜在威胁】安全报告中检查可调试组件扫描结果缺少组件名称 BUG #194823]
- 修复【潜在威胁】还原后删除潜在危险文件，再次扫描还原失败
- 修复导出的安全报告格式没有对齐，显示不美观
- 修复设置账户锁定项进行加固后，还原失败，ssh 密码验证失败

- 修复安全报告中，禁止/var/log 日志文件全局可读写描述信息未同步为可读写
- 修复设置守护进程的 umask 值该项进行加固后，再次扫描依然提示需要加固
- 修复系统环境满足无需加固，开启审计机制加固项仍显示待手动加固

- 修复限制日志文件权限设置更严格时，依然会被加固
- 修复限制 FTP 用户上传的文件所具有的权限更严格时，依然会被加固
- 修复限制重要目录或文件权限加固时，权限更严格依然会被加固
- 修复加固箱限制 SSH 服务可访问源
- 修复无法导出安全报告明细
- 修复检查不安全组件加固项详情描述中未添加组件名
- 修复【系统设置】设置系统引导管理器密码扫描结果为等待加固，重启系统进入 grub 依然需要输入密码
- 修复限制日志文件权限设置更严格时，依然会被加固
- 修复【非交互命令】未使用过安全加固可导出安全报告]
- 修复【系统审计】开启审计机制加固项还原失败，同时导致加固服务停止
- 修复设置账户登录失败锁定功能加固逻辑错误

- 修复当扫描过程存在对参数的判断时，参数值为空时扫描卡死
- 修复禁用 ctrl+alt+del 组合键后在 tty 界面重启，系统会卡住

- 因 tripwire 软件包不再维护，去掉检查文件系统和磁盘完整性校验加固项

9. 附录 5 iso 集成新增软件

- apache-commons-dbcp-1.4-26.ky10
- apache-commons-pool-1.6-19.ky10
- audit-status-libs-1.0.1-02.ky10
- autocorr-zh-6.4.7.2-13.p01.ky10
- gb-cjk-fonts-1.0.0-1.ky10
- git-core-2.33.0-12.ky10
- glib-1.2.10-57.ky10
- grub2-efi-aa64-trust-measure-modules-2.04-37.p10.se.11.ky10
- grub2-efi-x64-trust-measure-modules-2.04-37.p10.se.11.ky10
- gtk+-1.2.10-90.ky10
- gtksourceview4-4.8.1-1.ky10
- json-c-devel-0.15-6.ky10
- kylin-activation-ukey-driver-1.0-1.p01.ky10
- kylin-settings-mini-14.10.63-1s4.p13.ky10
- kylin-sysassist-1.3-1.ky10
- kylin-sysassist-db-1.3-1.ky10
- kysec-module-authorize-upgrade-1.0.0-1.se.04.ky10
- kytrust-bima-2.0.14-10.ky10
- libasan-7.3.0-2020033101.58.p01.ky10
- libatomic-7.3.0-2020033101.58.p01.ky10
- libgee-0.20.1-5.ky10
- libkysdk-module-authorize-1.0.0-02.ky10
- libkysec-module-authorize-1.0.0-1.se.04.ky10
- libkytrusted-security-1.0.1-10.ky10
- libldm-0.2.4-3.p01.ky10

- libpfm-help-4.12.0-1.p02.ky10
- libselinux-ruby-3.1-7.se.03.ky10
- libsm-devctl-1.0.1-15.ky10
- libsm-netflow-1.0.1-15.ky10
- libsm-safeguard-1.0.1-15.ky10
- libtcmalg-1.0-se.04.ky10
- libubsan-7.3.0-2020033101.58.p01.ky10
- libva-2.5.0-2.ky10
- poppler-utils-0.90.0-6.ky10
- python2-libselinux-3.1-7.se.03.ky10
- python2-libsemanage-3.1-3.se.02.ky10
- setools-4.3.0-4.ky10
- sm-enhancement-1.0.1-15.ky10
- sm-netflow-daemon-1.0.0-08.ky10
- tpm2-tss-devel-3.0.3-2.p01.ky10
- trousers-tcm-0.3.15-06.ky10
- trousers-tcm-tools-1.3.4-06.ky10

10. 附录 6 iso 集成减少软件

- cdrkit-help-1.1.11-43.ky10
- cesi-fonts-1.0.0-1.ky10
- dnsmasq-help-2.82-9.ky10
- libreoffice-base-6.3.6.2-3.p02.ky10
- libreoffice-calc-6.3.6.2-3.p02.ky10
- libreoffice-core-6.3.6.2-3.p02.ky10
- libreoffice-data-6.3.6.2-3.p02.ky10
- libreoffice-draw-6.3.6.2-3.p02.ky10
- libreoffice-emailmerge-6.3.6.2-3.p02.ky10

- libreoffice-graphicfilter-6.3.6.2-3.p02.ky10
- libreoffice-gtk3-6.3.6.2-3.p02.ky10
- libreoffice-help-en-6.3.6.2-3.p02.ky10
- libreoffice-impress-6.3.6.2-3.p02.ky10
- libreoffice-langpack-en-6.3.6.2-3.p02.ky10
- libreoffice-math-6.3.6.2-3.p02.ky10
- libreoffice-ogltrans-6.3.6.2-3.p02.ky10
- libreoffice-opensymbol-fonts-6.3.6.2-3.p02.ky10
- libreoffice-pdfimport-6.3.6.2-3.p02.ky10
- libreoffice-pyuno-6.3.6.2-3.p02.ky10
- libreoffice-ure-6.3.6.2-3.p02.ky10
- libreoffice-ure-common-6.3.6.2-3.p02.ky10
- libreoffice-wiki-publisher-6.3.6.2-3.p02.ky10
- libreoffice-writer-6.3.6.2-3.p02.ky10
- libreoffice-x11-6.3.6.2-3.p02.ky10
- zeromq-devel-4.1.7-2.ky10

11. 附录 7 安全漏洞修复

11.1. 内核漏洞修复清单(278 个)

CVE-2023-39197 CVE-2021-4204 CVE-2023-34324 CVE-2023-3863 CVE-2022-44033 CVE-2022-3176 CVE-2022-20568 CVE-2023-35827 CVE-2022-45884 CVE-2023-37453 CVE-2023-21400 CVE-2023-1295 CVE-2022-3903 CVE-2021-33639 CVE-2022-2991 CVE-2023-20588 CVE-2023-30456 CVE-2023-0160 CVE-2023-5717 CVE-2023-5178 CVE-2023-45871 CVE-2023-39189 CVE-2023-31085 CVE-2023-31083 CVE-2023-1206 CVE-2023-34319 CVE-2021-34866 CVE-2020-14356 CVE-2022-2905 CVE-2023-2163 CVE-2021-20268 CVE-2021-3489 CVE-2023-39192 CVE-2023-39193 CVE-2023-39194 CVE-2023-42754

CVE-2023-4134 CVE-2023-4133 CVE-2023-4881 CVE-2023-42753 CVE-2023-3772 CVE-2023-4622 CVE-2023-42752 CVE-2023-42755 CVE-2022-40982 CVE-2023-4563 CVE-2023-4921 CVE-2023-4623 CVE-2020-14356 CVE-2021-20268 CVE-2021-33639 CVE-2021-34866 CVE-2021-3489 CVE-2021-4204 CVE-2022-20568 CVE-2022-2905 CVE-2022-2991 CVE-2022-3176 CVE-2022-3903 CVE-2022-40982 CVE-2022-44033 CVE-2022-45884 CVE-2023-0160 CVE-2023-1206 CVE-2023-1295 CVE-2023-20588 CVE-2023-21400 CVE-2023-2163 CVE-2023-30456 CVE-2023-31083 CVE-2023-31085 CVE-2023-34319 CVE-2023-34324 CVE-2023-35827 CVE-2023-37453 CVE-2023-3772 CVE-2023-3863 CVE-2023-39189 CVE-2023-39192 CVE-2023-39193 CVE-2023-39194 CVE-2023-39197 CVE-2023-4133 CVE-2023-4134 CVE-2023-42752 CVE-2023-42753 CVE-2023-42754 CVE-2023-42755 CVE-2023-4563 CVE-2023-45871 CVE-2023-4622 CVE-2023-4623 CVE-2023-4881 CVE-2023-4921 CVE-2023-5178 CVE-2023-5717 CVE-2019-19036 CVE-2019-20794 CVE-2019-25044 CVE-2020-10751 CVE-2020-12114 CVE-2020-24504 CVE-2020-27784 CVE-2020-29372 CVE-2020-29374 CVE-2020-35499 CVE-2020-36691 CVE-2020-8835 CVE-2021-20194 CVE-2021-38166 CVE-2021-3923 CVE-2021-4001 CVE-2021-4218 CVE-2022-0480 CVE-2022-1280 CVE-2022-1462 CVE-2022-20369 CVE-2022-20422 CVE-2022-20423 CVE-2022-23816 CVE-2022-2503 CVE-2022-2586 CVE-2022-2588 CVE-2022-2602 CVE-2022-26373 CVE-2022-2663 CVE-2022-27672 CVE-2022-29582 CVE-2022-2964 CVE-2022-2977 CVE-2022-2978 CVE-2022-29900 CVE-2022-29901 CVE-2022-3028 CVE-2022-3061 CVE-2022-3105 CVE-2022-3107 CVE-2022-3108 CVE-2022-3111 CVE-2022-3115 CVE-2022-3169 CVE-2022-3202 CVE-2022-3239 CVE-2022-3303 CVE-2022-3424 CVE-2022-3521 CVE-2022-3524 CVE-2022-3535 CVE-2022-3542 CVE-2022-3545 CVE-2022-3564 CVE-2022-3565 CVE-2022-3566 CVE-2022-3567 CVE-2022-3594 CVE-2022-3621 CVE-2022-3628 CVE-2022-36280 CVE-2022-3629 CVE-2022-3633 CVE-2022-3635 CVE-2022-3640 CVE-2022-3643 CVE-2022-36

46 CVE-2022-3649 CVE-2022-3707 CVE-2022-39188 CVE-2022-39189 CVE-2022-39842 CVE-2022-40307 CVE-2022-40768 CVE-2022-4095 CVE-2022-41218 CVE-2022-4129 CVE-2022-41848 CVE-2022-41849 CVE-2022-41850 CVE-2022-41858 CVE-2022-42328 CVE-2022-42329 CVE-2022-42432 CVE-2022-4269 CVE-2022-42703 CVE-2022-42895 CVE-2022-42896 CVE-2022-43750 CVE-2022-4378 CVE-2022-45934 CVE-2022-4662 CVE-2022-4696 CVE-2022-47929 CVE-2023-0030 CVE-2023-0045 CVE-2023-0122 CVE-2023-0266 CVE-2023-0386 CVE-2023-0394 CVE-2023-0458 CVE-2023-0459 CVE-2023-0461 CVE-2023-0590 CVE-2023-0615 CVE-2023-1073 CVE-2023-1074 CVE-2023-1075 CVE-2023-1076 CVE-2023-1077 CVE-2023-1078 CVE-2023-1079 CVE-2023-1118 CVE-2023-1252 CVE-2023-1281 CVE-2023-1380 CVE-2023-1382 CVE-2023-1513 CVE-2023-1582 CVE-2023-1611 CVE-2023-1637 CVE-2023-1670 CVE-2023-1829 CVE-2023-1838 CVE-2023-1855 CVE-2023-1859 CVE-2023-1989 CVE-2023-1990 CVE-2023-2002 CVE-2023-2007 CVE-2023-20593 CVE-2023-20928 CVE-2023-20938 CVE-2023-2124 CVE-2023-2162 CVE-2023-2176 CVE-2023-2177 CVE-2023-2194 CVE-2023-2248 CVE-2023-2269 CVE-2023-23000 CVE-2023-23454 CVE-2023-23455 CVE-2023-23559 CVE-2023-2483 CVE-2023-2513 CVE-2023-26545 CVE-2023-26607 CVE-2023-28328 CVE-2023-28466 CVE-2023-2985 CVE-2023-30772 CVE-2023-3090 CVE-2023-31084 CVE-2023-3111 CVE-2023-3117 CVE-2023-3141 CVE-2023-3159 CVE-2023-3161 CVE-2023-3212 CVE-2023-3220 CVE-2023-32233 CVE-2023-32269 CVE-2023-3268 CVE-2023-33203 CVE-2023-33288 CVE-2023-3338 CVE-2023-3358 CVE-2023-34256 CVE-2023-35001 CVE-2023-3567 CVE-2023-35788 CVE-2023-35823 CVE-2023-35824 CVE-2023-35828 CVE-2023-3609 CVE-2023-3611 CVE-2023-3776 CVE-2023-40283 CVE-2023-4128 CVE-2023-4132

11.2. 核外漏洞修复清单（1010 个）

CVE-2023-30577 CVE-2022-37705 CVE-2023-24998 CVE-2021-37533 CVE-2022-45047

CVE-2022-24963 CVE-2022-25147 CVE-2022-47630 CVE-2023-1981 CVE-2023-38470 CVE-2023-38469 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473 CVE-2022-41704 CVE-2022-42890 CVE-2023-3341 CVE-2023-2828 CVE-2022-2906 CVE-2022-2881 CVE-2022-2795 CVE-2022-38178 CVE-2022-38177 CVE-2022-47008 CVE-2022-47011 CVE-2022-47696 CVE-2022-48064 CVE-2021-46174 CVE-2020-24240 CVE-2021-0129 CVE-2022-0204 CVE-2021-41229 CVE-2022-39176 CVE-2022-39177 CVE-2023-27349 CVE-2023-33201 CVE-2021-33641 CVE-2021-33642 CVE-2022-4904 CVE-2023-32067 CVE-2023-31130 CVE-2023-31124 CVE-2023-31147 CVE-2020-12059 CVE-2020-25678 CVE-2020-27781 CVE-2020-10753 CVE-2021-3524 CVE-2020-1760 CVE-2021-3979 CVE-2023-43040 CVE-2022-27239 CVE-2022-29869 CVE-2023-20032 CVE-2023-20052 CVE-2023-20197 CVE-2022-2084 CVE-2023-1786 CVE-2021-3660 CVE-2015-1197 CVE-2021-38185 CVE-2020-14382 CVE-2022-4515 CVE-2023-24805 CVE-2022-26691 CVE-2019-8842 CVE-2023-32324 CVE-2023-34241 CVE-2023-4504 CVE-2023-32001 CVE-2023-38545 CVE-2023-38546 CVE-2023-28320 CVE-2023-28321 CVE-2023-28322 CVE-2023-27536 CVE-2023-27535 CVE-2023-27533 CVE-2023-27534 CVE-2023-27538 CVE-2023-23916 CVE-2022-32221 CVE-2022-35252 CVE-2022-24407 CVE-2022-42010 CVE-2023-34969 CVE-2005-1849 CVE-2016-9840 CVE-2016-9841 CVE-2016-9843 CVE-2018-25032 CVE-2022-37434 CVE-2021-25214 CVE-2021-25215 CVE-2021-25219 CVE-2021-25220 CVE-2022-2928 CVE-2022-2929 CVE-2021-46310 CVE-2021-46312 CVE-2023-30630 CVE-2020-25681 CVE-2020-25682 CVE-2020-25683 CVE-2020-25684 CVE-2020-25685 CVE-2020-25686 CVE-2020-25687 CVE-2021-3448 CVE-2023-25173 CVE-2023-25153 CVE-2023-28840 CVE-2022-24769 CVE-2022-36109 CVE-2023-28841 CVE-2023-28842 CVE-2022-29162 CVE-2020-28200 CVE-2021-33515 CVE-2022-30550 CVE-2020-11022 CVE-2020-11023 CVE-2020-23064 CVE-2019-14584 CVE-2019-11098 CVE-2021-38578 CVE-2022-4450 CVE-2023-0401 CVE-2023-0215 CVE-2023-0286 CVE-2022-4304 CVE-2021-33294 CVE-2022-45939 CVE-2022-48337 CVE-2022-48338 CVE-2022-48339 CVE-2023-28617 CVE-2020-14928 CVE-2020-18651 CVE-2020-18652 CVE-2021-36048 CVE-2021-39847 CVE-2021-42530 CVE-2021-36046 CVE-2021-36055 CVE-2021-40716 CVE-2018-12648 CVE-2021-36054 CVE-2021-36047 CVE-2021-36052 CVE-2021-36058 CVE-2021-36045 CVE-2021-42531 CVE-2021-36064 CVE-2021-42529 CVE-2021-42528 CVE-2021-36050 CVE-2021-40732 CVE-2021-36056 CVE-2021-42532 CVE-2021-36053 CVE-2021-36051 CVE-2019-13108 CVE-2019-13504 CVE-2021-31292 CVE-2021-32815 CVE-2021-37620 CVE-2021-37619 CVE-2021-34335 CVE-2021-

37618 CVE-2021-37621 CVE-2021-34334 CVE-2021-37622 CVE-2021-37623 CVE-2021-37615 CVE-2021-37616 CVE-2022-3755 CVE-2022-3756 CVE-2022-25235 CVE-2022-25236 CVE-2022-25313 CVE-2022-25314 CVE-2022-25315 CVE-2022-40674 CVE-2022-43680 CVE-2021-38114 CVE-2020-35964 CVE-2020-15969 CVE-2020-15999 CVE-2020-16012 CVE-2020-26953 CVE-2020-26957 CVE-2020-26958 CVE-2020-26959 CVE-2020-26960 CVE-2020-26961 CVE-2020-26965 CVE-2020-26967 CVE-2023-23606 CVE-2022-22755 CVE-2022-22827 CVE-2023-4863 CVE-2023-5217 CVE-2023-7104 CVE-2021-21417 CVE-2022-41860 CVE-2022-41861 CVE-2022-39320 CVE-2022-39317 CVE-2022-39316 CVE-2022-39318 CVE-2022-39319 CVE-2022-39347 CVE-2022-41877 CVE-2022-39282 CVE-2022-24882 CVE-2022-24883 CVE-2022-27404 CVE-2022-27405 CVE-2022-27406 CVE-2023-2004 CVE-2022-40899 CVE-2023-4039 CVE-2023-39130 CVE-2023-39129 CVE-2023-39128 CVE-2021-20240 CVE-2020-29385 CVE-2021-46829 CVE-2021-44648 CVE-2023-43115 CVE-2023-36664 CVE-2023-28879 CVE-2023-38559 CVE-2022-28506 CVE-2023-39742 CVE-2022-39260 CVE-2022-23521 CVE-2022-41903 CVE-2023-5156 CVE-2023-4806 CVE-2023-4813 CVE-2022-48340 CVE-2023-26253 CVE-2018-17942 CVE-2022-34903 CVE-2020-25969 CVE-2022-2509 CVE-2021-4209 CVE-2023-0361 CVE-2023-5981 CVE-2023-24539 CVE-2023-24540 CVE-2023-29400 CVE-2023-29402 CVE-2023-29403 CVE-2023-29404 CVE-2023-29405 CVE-2023-29406 CVE-2023-29409 CVE-2023-39318 CVE-2023-39319 CVE-2023-39323 CVE-2023-39325 CVE-2023-39326 CVE-2022-24921 CVE-2022-23773 CVE-2022-28327 CVE-2022-24675 CVE-2021-44717 CVE-2022-32148 CVE-2022-1962 CVE-2022-1705 CVE-2022-30633 CVE-2022-30635 CVE-2022-30632 CVE-2022-28131 CVE-2022-30631 CVE-2022-30629 CVE-2022-30634 CVE-2022-32189 CVE-2022-29804 CVE-2022-29526 CVE-2022-27664 CVE-2022-41715 CVE-2022-2880 CVE-2022-2879 CVE-2022-41716 CVE-2022-41717 CVE-2022-41723 CVE-2022-41724 CVE-2022-41725 CVE-2023-24534 CVE-2023-24536 CVE-2023-24537 CVE-2023-24538 CVE-2023-45285 CVE-2022-25647 CVE-2023-4785 CVE-2021-3981 CVE-2021-3697 CVE-2022-28735 CVE-2022-28736 CVE-2022-28734 CVE-2022-28733 CVE-2021-3695 CVE-2021-3696 CVE-2022-2601 CVE-2022-3775 CVE-2023-4692 CVE-2023-4693 CVE-2023-25567 CVE-2023-25564 CVE-2023-25563 CVE-2023-25565 CVE-2022-2122 CVE-2022-1920 CVE-2022-2121 CVE-2022-1922 CVE-2022-1923 CVE-2022-1924 CVE-2022-1925 CVE-2021-3497 CVE-2021-3498 CVE-2023-2976 CVE-2023-25725 CVE-2023-0056 CVE-2023-40225 CVE-2023-0836 CVE-2023-45539 CVE-2022-33068 CVE-2023-25193 CVE-2018-13867 CVE-2018-14031 CVE-2018-16438

CVE-2019-8396 CVE-2020-10812 CVE-2021-37501 CVE-2018-14033 CVE-2018-14460 CVE-2020-10811 CVE-2020-10810 CVE-2021-32765 CVE-2022-22719 CVE-2022-22720 CVE-2022-22721 CVE-2022-23943 CVE-2022-29404 CVE-2022-30556 CVE-2022-28614 CVE-2022-26377 CVE-2022-30522 CVE-2022-28615 CVE-2022-31813 CVE-2022-28330 CVE-2022-36760 CVE-2006-20001 CVE-2022-37436 CVE-2023-25690 CVE-2023-27522 CVE-2019-17567 CVE-2023-31122 CVE-2023-45802 CVE-2022-29486 CVE-2023-28711 CVE-2022-1115 CVE-2022-3213 CVE-2022-32547 CVE-2022-44267 CVE-2022-44268 CVE-2023-1289 CVE-2023-1906 CVE-2023-34151 CVE-2023-3428 CVE-2023-39978 CVE-2023-40305 CVE-2022-2068 CVE-2022-0778 CVE-2022-1292 CVE-2022-2097 CVE-2023-38403 CVE-2023-22081 CVE-2023-22006 CVE-2023-22036 CVE-2023-22041 CVE-2023-22044 CVE-2023-22045 CVE-2023-22049 CVE-2023-21930 CVE-2023-21937 CVE-2023-21938 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968 CVE-2023-21835 CVE-2023-21843 CVE-2022-21618 CVE-2022-21619 CVE-2022-21626 CVE-2022-21624 CVE-2022-21628 CVE-2022-39399 CVE-2022-21540 CVE-2022-21541 CVE-2022-34169 CVE-2022-21426 CVE-2022-21443 CVE-2022-21434 CVE-2022-21496 CVE-2022-21248 CVE-2022-21283 CVE-2022-21291 CVE-2022-21293 CVE-2022-21294 CVE-2022-21282 CVE-2022-21296 CVE-2022-21299 CVE-2022-21277 CVE-2022-21305 CVE-2022-21340 CVE-2022-21341 CVE-2022-21360 CVE-2022-21365 CVE-2022-21366 CVE-2022-21476 CVE-2022-21349 CVE-2023-21830 CVE-2023-22067 CVE-2019-10241 CVE-2022-2047 CVE-2022-2048 CVE-2021-32292 CVE-2023-1370 CVE-2021-20269 CVE-2023-36054 CVE-2022-42898 CVE-2022-46663 CVE-2021-36976 CVE-2022-36227 CVE-2023-2603 CVE-2022-40320 CVE-2020-27545 CVE-2020-28163 CVE-2020-0452 CVE-2019-9278 CVE-2020-0181 CVE-2020-0198 CVE-2020-0093 CVE-2020-12762 CVE-2019-13627 CVE-2022-47629 CVE-2022-3515 CVE-2023-26769 CVE-2022-26981 CVE-2022-31783 CVE-2023-26767 CVE-2023-26768 CVE-2023-27371 CVE-2019-15161 CVE-2019-15162 CVE-2019-15163 CVE-2019-15164 CVE-2019-15165 CVE-2020-25219 CVE-2023-35789 CVE-2023-1729 CVE-2023-38710 CVE-2023-38711 CVE-2023-38712 CVE-2023-38633 CVE-2021-36084 CVE-2021-36086 CVE-2021-36085 CVE-2021-36087 CVE-2021-3200 CVE-2021-44568 CVE-2021-44569 CVE-2021-44571 CVE-2021-44573 CVE-2021-44574 CVE-2021-44575 CVE-2021-44576 CVE-2021-44577 CVE-2023-1667 CVE-2023-2283 CVE-2021-33643 CVE-2021-33644 CVE-2021-33645 CVE-2021-33646 CVE-2021-46848 CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2022-3597 CVE-2022-3527 CVE-2022-3526 CVE-2022-3570 CVE-2022-3598 CVE-2022-3599

CVE-2022-3970 CVE-2022-48281 CVE-2023-0795 CVE-2023-0796 CVE-2023-0798 CVE-2023-0799 CVE-2023-0800 CVE-2023-0802 CVE-2023-0803 CVE-2023-0804 CVE-2023-0797 CVE-2023-0801 CVE-2023-2731 CVE-2023-26965 CVE-2023-3316 CVE-2023-25433 CVE-2023-26966 CVE-2023-2908 CVE-2023-3576 CVE-2023-38288 CVE-2023-38289 CVE-2023-3618 CVE-2022-40090 CVE-2022-34526 CVE-2023-6228 CVE-2023-6277 CVE-2020-29260 CVE-2023-1999 CVE-2022-3554 CVE-2022-3555 CVE-2023-3138 CVE-2023-43785 CVE-2023-43786 CVE-2023-43787 CVE-2023-45322 CVE-2023-28484 CVE-2023-29469 CVE-2022-40303 CVE-2022-40304 CVE-2016-3709 CVE-2022-29824 CVE-2022-23308 CVE-2022-44617 CVE-2022-46285 CVE-2022-4883 CVE-2021-30560 CVE-2021-44832 CVE-2022-47925 CVE-2018-3282 CVE-2018-3174 CVE-2018-3143 CVE-2018-3156 CVE-2018-3251 CVE-2018-3185 CVE-2018-3277 CVE-2018-3162 CVE-2018-3173 CVE-2018-3200 CVE-2018-3284 CVE-2019-2510 CVE-2019-2537 CVE-2019-2614 CVE-2019-2627 CVE-2019-2805 CVE-2019-2740 CVE-2019-2739 CVE-2019-2737 CVE-2019-2758 CVE-2020-2922 CVE-2021-2007 CVE-2019-2974 CVE-2019-2938 CVE-2020-2780 CVE-2021-2144 CVE-2020-2752 CVE-2020-2812 CVE-2020-2814 CVE-2020-2760 CVE-2020-13249 CVE-2021-2022 CVE-2020-15180 CVE-2020-14812 CVE-2020-14765 CVE-2020-14776 CVE-2020-14789 CVE-2020-28912 CVE-2021-2194 CVE-2021-27928 CVE-2021-2166 CVE-2021-2154 CVE-2022-21451 CVE-2021-2372 CVE-2021-2389 CVE-2021-46658 CVE-2021-35604 CVE-2021-46667 CVE-2021-46662 CVE-2022-27385 CVE-2022-31624 CVE-2022-24052 CVE-2022-24051 CVE-2022-24050 CVE-2022-24048 CVE-2021-46659 CVE-2022-21595 CVE-2021-46665 CVE-2021-46664 CVE-2021-46661 CVE-2021-46668 CVE-2021-46663 CVE-2023-5157 CVE-2022-32091 CVE-2022-32084 CVE-2022-38791 CVE-2022-47015 CVE-2022-40982 CVE-2022-38090 CVE-2022-33196 CVE-2023-23583 CVE-2022-2255 CVE-2022-41974 CVE-2023-4874 CVE-2023-4875 CVE-2022-1328 CVE-2020-14954 CVE-2022-44370 CVE-2020-21528 CVE-2023-29491 CVE-2022-24805 CVE-2022-24806 CVE-2022-24807 CVE-2022-24808 CVE-2022-24809 CVE-2022-24810 CVE-2022-44792 CVE-2022-44793 CVE-2023-44487 CVE-2023-35945 CVE-2022-41742 CVE-2022-41741 CVE-2019-9511 CVE-2019-9513 CVE-2019-9516 CVE-2021-23017 CVE-2022-43548 CVE-2022-40284 CVE-2020-15025 CVE-2023-26551 CVE-2023-26552 CVE-2023-26553 CVE-2023-26554 CVE-2023-26555 CVE-2022-29155 CVE-2023-2953 CVE-2021-42780 CVE-2021-42782 CVE-2023-2977 CVE-2023-40660 CVE-2023-40661 CVE-2023-38408 CVE-2023-51385 CVE-2023-48795 CVE-2023-5678 CVE-2023-3817 CVE-2023-3446 CVE-2023-2650 CVE-2023-0464 CVE-2015

-8011 CVE-2020-27827 CVE-2020-35498 CVE-2022-4338 CVE-2023-1668 CVE-2023-5366 CVE-2022-47021 CVE-2020-27780 CVE-2022-1586 CVE-2022-1587 CVE-2021-36770 CVE-2023-31486 CVE-2023-31484 CVE-2022-3560 CVE-2022-44638 CVE-2023-24056 CVE-2023-41915 CVE-2021-4115 CVE-2022-27337 CVE-2022-37050 CVE-2022-37051 CVE-2022-37052 CVE-2022-38349 CVE-2020-23804 CVE-2020-36023 CVE-2022-41946 CVE-2021-20229 CVE-2021-32028 CVE-2022-4603 CVE-2023-4016 CVE-2019-18217 CVE-2021-46854 CVE-2022-33070 CVE-2021-22570 CVE-2019-20907 CVE-2021-4189 CVE-2022-0391 CVE-2015-20107 CVE-2021-28861 CVE-2020-10735 CVE-2022-37454 CVE-2023-24329 CVE-2022-23491 CVE-2023-37920 CVE-2023-23931 CVE-2021-21240 CVE-2022-21797 CVE-2022-2309 CVE-2022-24302 CVE-2022-22815 CVE-2022-22816 CVE-2022-45198 CVE-2023-44271 CVE-2022-45199 CVE-2022-24303 CVE-2021-23437 CVE-2020-14422 CVE-2021-33503 CVE-2023-33733 CVE-2020-28463 CVE-2023-32681 CVE-2022-40897 CVE-2023-28370 CVE-2023-43804 CVE-2023-45803 CVE-2023-23934 CVE-2023-25577 CVE-2023-2861 CVE-2023-0664 CVE-2023-3180 CVE-2023-3354 CVE-2020-24165 CVE-2020-13791 CVE-2021-3638 CVE-2022-35414 CVE-2021-3507 CVE-2021-20257 CVE-2020-13253 CVE-2021-3607 CVE-2021-3608 CVE-2022-0216 CVE-2022-4144 CVE-2022-1050 CVE-2023-24607 CVE-2023-32762 CVE-2023-32763 CVE-2023-37369 CVE-2023-33285 CVE-2023-34410 CVE-2023-38197 CVE-2023-43114 CVE-2021-45930 CVE-2023-32573 CVE-2020-0570 CVE-2020-17507 CVE-2021-32626 CVE-2021-29478 CVE-2021-32672 CVE-2022-36021 CVE-2023-28856 CVE-2021-35937 CVE-2021-35939 CVE-2021-35938 CVE-2022-29154 CVE-2022-24903 CVE-2022-24836 CVE-2023-36617 CVE-2023-28755 CVE-2023-28756 CVE-2021-33621 CVE-2022-32743 CVE-2022-3437 CVE-2022-44640 CVE-2022-45141 CVE-2022-38023 CVE-2023-0922 CVE-2022-2127 CVE-2023-34966 CVE-2023-34967 CVE-2023-4091 CVE-2023-42669 CVE-2023-24626 CVE-2022-4743 CVE-2013-4235 CVE-2023-4641 CVE-2023-29383 CVE-2017-3735 CVE-2017-3737 CVE-2018-0732 CVE-2018-0739 CVE-2019-1563 CVE-2020-1971 CVE-2021-23841 CVE-2021-3712 CVE-2022-41854 CVE-2022-25857 CVE-2022-38749 CVE-2022-38750 CVE-2022-38751 CVE-2022-38752 CVE-2023-34454 CVE-2023-34455 CVE-2023-43642 CVE-2021-33844 CVE-2023-32627 CVE-2021-23159 CVE-2023-34432 CVE-2023-34318 CVE-2021-23172 CVE-2021-3643 CVE-2021-23210 CVE-2022-31650 CVE-2023-26590 CVE-2022-31651 CVE-2017-18189 CVE-2023-32697 CVE-2021-46784 CVE-2022-41317 CVE-2022-41318 CVE-2023-46846 CVE-2023-46847 CVE-2023-46724 CVE-2023-46728 CVE-2023-49285 CVE-2023-49286 CVE-2023-50269

CVE-2022-40617 CVE-2023-42465 CVE-2022-43995 CVE-2023-22809 CVE-2023-2848
6 CVE-2023-28487 CVE-2022-39377 CVE-2023-33204 CVE-2022-3821 CVE-2023-2660
4 CVE-2023-1672 CVE-2023-39804 CVE-2021-35331 CVE-2023-1801 CVE-2023-32700
CVE-2023-1393 CVE-2023-22745 CVE-2023-46316 CVE-2022-30767 CVE-2022-34835
CVE-2022-3204 CVE-2022-30698 CVE-2022-30699 CVE-2023-1108 CVE-2023-2609 C
VE-2023-2610 CVE-2023-2426 CVE-2023-1264 CVE-2023-1170 CVE-2023-1175 CVE-
2023-0433 CVE-2022-47024 CVE-2023-0288 CVE-2023-0049 CVE-2023-0051 CVE-202
3-0054 CVE-2022-4292 CVE-2022-4293 CVE-2022-3491 CVE-2022-3520 CVE-2022-35
91 CVE-2022-4141 CVE-2022-3705 CVE-2022-3324 CVE-2022-3297 CVE-2022-3296 C
VE-2022-3352 CVE-2022-0135 CVE-2022-0175 CVE-2021-3782 CVE-2023-28204 CVE
-2022-2319 CVE-2022-2320 CVE-2022-3551 CVE-2022-3553 CVE-2022-4283 CVE-202
2-46340 CVE-2022-46341 CVE-2022-46342 CVE-2022-46343 CVE-2022-46344 CVE-20
23-0494 CVE-2022-3550 CVE-2023-5367 CVE-2023-5380 CVE-2023-6478 CVE-2023-6
377 CVE-2022-24795 CVE-2023-37732 CVE-2023-45853 CVE-2020-18770 CVE-2022-3
625 CVE-2020-35728 CVE-2022-42012 CVE-2022-42011 CVE-2022-39253 CVE-2022-4
1853 CVE-2022-4603 CVE-2022-42252 CVE-2022-41953 CVE-2022-41973 CVE-2022-2
5881 CVE-2023-22490 CVE-2023-23946 CVE-2022-48303 CVE-2022-47952 CVE-2022-
37704 CVE-2023-28708 CVE-2023-24593 CVE-2023-25180 CVE-2023-29007 CVE-2023
-25652 CVE-2023-30570 CVE-2023-25815 CVE-2022-3171 CVE-2022-1941 CVE-2023-
30861 CVE-2023-2856 CVE-2022-48565 CVE-2022-48566 CVE-2023-39356 CVE-2022-
48174 CVE-2023-39352 CVE-2023-40186 CVE-2023-40188 CVE-2023-40569 CVE-2023
-40589 CVE-2023-39354 CVE-2023-39351 CVE-2023-39350 CVE-2023-39353 CVE-202
3-40181 CVE-2023-40567 CVE-2023-23918 CVE-2023-23920 CVE-2023-30581 CVE-20
23-30590 CVE-2023-32006 CVE-2023-32002 CVE-2023-3823 CVE-2023-3824 CVE-202
3-0662 CVE-2023-41080 CVE-2023-40217 CVE-2023-27043 CVE-2023-45648 CVE-202
3-28450 CVE-2023-32559 CVE-2023-4738 CVE-2023-4752 CVE-2023-4750 CVE-2023-
4733 CVE-2023-4736 CVE-2023-4735 CVE-2023-4734 CVE-2023-4781 CVE-2023-5344
CVE-2023-5535 CVE-2023-5441 CVE-2023-48706 CVE-2023-46246 CVE-2023-30589
CVE-2022-40151 CVE-2023-45866 CVE-2023-6121 CVE-2023-46218 CVE-2023-37327
CVE-2023-22742 CVE-2023-44442 CVE-2023-6004 CVE-2023-44444 CVE-2022-41966
CVE-2023-5341 CVE-2022-4065 CVE-2024-23301 CVE-2023-35887 CVE-2022-26592 C
VE-2022-43358 CVE-2022-43357 CVE-2021-33391 CVE-2022-40898 CVE-2023-0437 C
VE-2022-40023 CVE-2021-25786 CVE-2023-50229 CVE-2024-0727 CVE-2024-22211 C

VE-2023-51042 CVE-2023-6931 CVE-2024-0340 CVE-2023-51043 CVE-2023-46343 CV
E-2024-23849 CVE-2023-36328 CVE-2024-24806 CVE-2024-24577 CVE-2023-3966