KYLINSOFT
麒麟软件

银河麒麟高级服务器操作系统

V11 2503 发布说明

麒麟软件有限公司

2025 年 7 月

商标声明

KYLINSOFT 麒麟软件和其他麒麟商标均为麒麟软件有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受麒麟软件有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，麒麟软件有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容有可能变更，麒麟软件有限公司保留在没有任何通知或提示的情况下对内容进行修改的权利。除非另有约定，本文档仅作为使用指导，并不确保手册内容完全没有错误。本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目　录

1 概述

银河麒麟高级服务器操作系统 V11 2503，作为麒麟软件有限公司推出的新一代服务器级操作系统，具备多计算架构兼容能力，能够为各类服务器应用场景提供稳定可靠、高性能且安全合规的底层操作系统支撑。

本文档为银河麒麟高级服务器操作系统 V11 2503 的发布说明，系统性地阐述了版本迭代中的新增特性、功能优化升级及已知缺陷修复等核心发布信息，旨在清晰、准确地向用户说明本版本的具体更新情况。

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 V11
发布格式	ISO、虚拟机镜像、容器镜像、仓库源
版本查询方式	终端：使用 nkvers 指令查询 图形界面：设置-系统-关于

repo 源列表：

名称	描述
https://update.kylinos.cn/NS/V11/2503/os/adv/lic/base	base 仓库，存放基础软件包
https://update.kylinos.cn/NS/V11/2503/os/adv/lic/update	update 仓库，存放升级软件包
https://update.kylinos.cn/NS/V11/2503/hotpatch_update/	热补丁仓库，存放发布的热补丁包
https://busi-eco.kylinos.cn/NS/V11/2503	第三方商业仓库，存放第三方商业软件包
https://eps-server.openkylin.top/NS/V11/2503/EPKL/	第三方开源仓库，存放第三方开源软件包

3 技术参数

类型	参数信息
支持架构	AArch64、x86_64、LoongArch64
支持处理器型号	飞腾、鲲鹏、龙芯、海光、兆芯、Intel、AMD
支持固件类型	BIOS/UEFI
内核版本	6.6.0

Glibc版本	2.38
GCC版本	12.3.1
Java版本	1.8.0.452.b09、11.0.27.6、17.0.15.6、21.0.7.6
开发语言支持	C/C++、Java、Go、Python、Php、Perl、ruby等
桌面环境	UKUI 4
中文支持	GB18030-2022
虚拟化	KVM、qemu
授权方式	在线、离线、KMS机制；产品订阅
补丁更新	每周
客户群体	全行业用户

4 主要更新

- 架构支持
  - 飞腾：FT-2000+/64、S2500、S5000C、S5000C-E；
  - 鲲鹏：KP920、KP920 V200；
  - 龙芯：3C5000L、3C5000、3D5000、3C6000/S、3C6000/D、3C6000/Q；
  - 海光：海光 2 号、C86-3G，C86-4G；
  - 兆芯：KH-30000、KH-40000；
  - Intel：志强四代、五代、六代；
  - AMD：EPYC 处理器。
- 板卡适配
  - RAID 卡：广州领芯科技、飞鱼星、华为鲲鹏、众星微、Broadcom、Marvell Microchip、云芯智联等；
  - 网卡：Intel、Mellanox、Broadcom、网迅、楠菲、沐创、芯启源 nfp、北中网芯、众星微、云脉芯联、大普微网卡（x86_64、aarch64）等；
  - 显卡：709 GP201/202（ARM）、景嘉微 JM9 系列（ARM）、AMD 等；
  - 光纤卡：Broadcom、Marvell、Emulex、众星微等；

- NVMe 卡：三星、Intel、金泰克 Kimtigo、联芸 Maxio；
- BMC：AST、浪潮自研 BMC、龙芯 2k0500、海思 bmc、飞腾 BMC；
- 可信驱动：TCM2.0、TPM2.0。

● 专项适配国产硬件特性，包括鲲鹏 VirtCCA 机密虚拟机技术、海光 CSV1/2/3 安全虚拟化技术、飞腾虚机热迁移等。

● 优化内存管理：以复合页 folio 替代传统 page 管理，移除不必要复合页转换，减少 LRU 链表数量，提升内存回收效率并降低碎片化。

● 支持 EEVDF 调度器，显著改善延迟敏感型任务（如实时任务、交互式任务）的响应性和确定性；

● 支持 sched_ext 可编程调度：基于 eBPF 实现用户态动态编写调度策略，提供极致的可扩展性和灵活性。

● MPTCP 多路径全量特性支持：允许应用程序使用多个网络路径进行并行数据传输，智能地将流量分配至不同传输路径，提高数据传输的可靠性和吞吐量。

● dm vdo 去重和压缩功能特性支持：通过在块存储层透明地实现高级数据缩减功能，显著提升物理存储利用率。

● bcachefs 文件系统全量特性支持，提供企业级存储解决方案，适用于数据库虚拟化及大规模存储场景。

● 新增 kalert 智能故障预警框架：通过统一的内核故障预警框架来解决故障上报的零散性、极端性、易忽略性等，以实现故障上报、故障监测和故障管理的统一性。

● 支持 ketones 内核观察 ebpf 工具集：提供多个监控和可观测性工具，作为 BCC 的简化替代方案，提供增强的内核可观测性能力。

● 支持 netmaster 网络故障定位 ebpf 工具集：包括网络报文跟踪、网络故障诊断、网络丢包监测功能，帮助用户快速分析、定位网络问题。

● 优化大页场景下的内存水位线预留：以支持透明大页的使用需求，达到自适应调节预留内存的情况，释放内存给业务端使用。

● 支持 xfs 文件缓存并发写：支持对单个文件的缓存并发写入特性，大幅提升多

进程对单文件缓存写入性能。。

● 支持 xfs 全新 AF 空间分配算法：提供一种全新的空间分配算法，增加 xfs 在极度碎片化的情况下的空间利用率。

● 新增 sock 多路转发功能：针对网络转发应用场景，在内核 socket 层直接实现网络报文转发，优化报文转发路径，减少数据拷贝开销，提升网络转发效率，支持传输层协议的转换以及一对多的网络转发模型，满足高并发、低延迟的网络转发需求。

● 新增缓存 IO 亲和功能：在飞腾 S5000C 平台上，优先使用设备所在节点内存，降低跨 die 率，提升性能。

● GRUB 2 引导程序扩展 UEFI 动态内存管理，提升启动效率；新增 PCI/MMIO UART 支持增强兼容性；优化 loongarch64 平台 initramfs 加载能力；新增 KYLIN_ROOT_USE_UUID 配置项，支持根分区优先使用 UUID 标识。

● Shim 安全启动器默认开启 sbat 防回滚功能，强化启动链安全性；支持 x86_64/aarch64/loongarch64 平台安全启动认证。

● glibc 核心运行时库：malloc 引入 hugetlb 大页分配，支持场景化性能调优；新增 Safe-Linking 机制防护堆指针劫持攻击；AArch64 支持 ARMv8.5-a 分支保护；x86 平台通过 AVX2 指令优化 strstr/memset 函数性能；libpthread/libdl 等库并入 libc，简化升级。

● OpenJDK8 进行海光/兆芯 CPU 深度优化；C2 编译器支持 AVX512 指令集；新引入 OpenJDK 21。

● systemd 系统管理器：新增僵尸进程回收与关键进程自愈机制；蓝屏故障显示二维码诊断；集成 systemd-storagetm 块设备共享工具；支持 eBPF 程序编译。

● 兼容 NVIDIA 等主流算力平台的软件栈，为用户提供高效的开发运行环境，全面支持各种 AI 平台，实现 AI 软件栈全栈兼容：

  ■ 支持 CUDA、oneAPI 等 AI 平台框架；

  ■ 支持 PyTorch、TensorFlow 等训练框架，支持 Numpy、XGBoost、libxsmm 等基础算法库，确保 AI 应用在麒麟系统上高效开发与运行；

- 支持 vllm、llamacpp、transformers、国产 chitu、dynamo 等模型推理应用，支持 llamafactory、unsloth 等模型微调应用，全方面使能大模型应用开发；
- 支持 deepseek 开源周特性本地部署，包括高性能分布式存储文件系统 3fs、smallpond 套件、开源计算优化库 FlashMLA、DeepGEMM、EPLB、DualPipe。
- 支持 deepseek 开源周特性容器化部署，提供基于本次发布麒麟系统根容器镜像构建的容器镜像，包括高性能分布式存储文件系统 3fs 容器镜像以及 DeepSeek 开源特性增强容器镜像；
- 支持 opencv、oneDNN、ComputeLibrary 等计算机视觉库，支持 dlib、octave、libsvm 等 AI 数学库，构建完整的 AI 开发者生态。

● 提供基于本次发布麒麟系统根容器镜像构建的 CUDA、PyTorch、TensorFlow、vllm、chitu、llamacpp、llamafactory、unsloth、dynamo 等容器镜像，通过容器镜像天然的封装形式，提供开箱即用的使用体验。

注意：以上容器镜像不属于本产品发布组件，不提供商业技术支持

注意：容器镜像集成的 CUDA、Pytorch、Tensorflow、vllm、chitu、llamacpp、llamafactory、unsloth、dynamo、3FS 等组件及其相关依赖，来自于对应官方发布组件，与 OS 集成提供的软件包版本存在差异

● 支持 AI 应用工具 kyCopilot，通过调用大模型及使用 RAG 技术，提供自然语言问答与辅助编程功能，显著提升用户在麒麟操作系统上的工作效率，大幅降低系统使用难度与开发门槛。

● 安全框架全新升级为 Kysec 2.0，扩展 LSM 形成 KSAF 可编程访问控制框架，实现了分层解耦的内核安全访问控制架构，支持定制灵活的管控策略定义，实现对应用程序和资源访问权限管控以支持更多的安全接口，并允许其他模块在核外共同使用

● 身份认证提供基于证书的 UKEY 本地和远程双因子登录认证，提高系统边界安全。完善全栈国密，strongswan、gnutls、crypto-policies、openssl 等增加国密支持，并在工具中增加基于国密算法的使用。

● PostgreSQL 数据库：支持超 1GB 大表存储；内存/磁盘排序性能优化；修复关系截断导致的数据损坏风险；强化 libpq 字符串处理；修复 CVE-2024-10979 漏洞

（PL/Perl 环境变量越权修改）。

● kylin-sysassist 智能运维助手：一键全量/选择性日志采集，降低技术门槛，提升效率；自动检测系统漏洞/缺陷/不合理配置，提供修复方案；检查关键服务状态及内核调试参数；进程（CPU/内存/状态/信号）、内存（泄漏/回收）、存储（文件句柄/inode）、网络（数据包）多维监控；智能分析进程资源瓶颈（核内外内存/火焰图可视化）、网络问题（丢包/延时/IP 转换）。

● kynetobser 网络故障分析技术工具：利用 ebpf 技术分别收集被监控节点协议栈各层流量信息并可将节点收集的信息进行统一分析。

● exmonitor 应用性能监控：实时追踪应用性能指标异常，联动系统资源（CPU/内存/进程/网络/磁盘）监控；僵尸进程检测、网卡带宽利用率分析、磁盘时延告警，多维度关联定位根因。

● 存储 IO 诊断工具：eBPF 监控文件系统调用，实时输出元数据操作（时间/进程/PID/文件路径）；块层 IO 追踪：捕获读写位置/大小/类型，支持进程级数据活跃度统计；日志归档+实时打印双模式，快速定位 IO 性能故障。

● 文件系统元数据监控：专为 iSCSI 设计，监控 XFS/EXT4 文件系统关键元数据破坏行为；记录直接写入/缓存写入事件，关联进程 ID/内核调用栈，实时 syslog 告警。

● kyupgrade 原地升级工具：支持银河麒麟高级服务器操作系统 V10 系列产品在不重新部署业务应用的情况下原地升级到 V11 2503。

● kylin-pkgchecker 兼容性分析工具：支持软件包/系统级兼容性分析；检测维度：ABI/API 变更、包依赖/命令/服务/配置差异、动态库接口差异；输出 HTML 可视化报告+CSV 接口差异数据，支持本地同名包版本对比。

● kycompatguard 兼容性守护工具：守护已安装应用兼容性，阻断 dnf/yum 变更引发的兼容性破坏；支持 rpm/tar/tar.gz/zip 目录形式程序包分析，集成包管理器实时防护。

● kylin-warm 热补丁系统：标准化配置文件驱动热补丁制作，支持 6.6 内核（x86/ARM/龙芯）及 glibc/qemu/openssl；创新热补丁顺序控制引擎，确保加载/激活/卸载过程安全可靠；新增内核模块依赖检查、符号冲突校验、被替换模块检测三重防护机制。

● extuner 场景调优工具：全量采集 CPU/内存/磁盘/网络/日志数据，输出 HTML 性能瓶颈报告；内置大数据/数据库/中间件等场景专家参数库，支持一键下发；AI 智能调优：通过函数拟合推导最优参数组合，加密混淆技术保护调优方案。

● kyldop 动态调优工具：基于 netlink 监控进程生命周期，按需实施环境变量/sysctl 参数优化；国密算法加密方案，支持无损回滚机制，确保调优安全可控。

● 系统授权激活组件增强：新增产品密钥激活、客户端取消激活、跨产品架构授权功能；完成与 KMS 2.5 的兼容适配；修复内存泄漏、KMS 广播激活失败等关键问题。

● 支持产品订阅：支持在线场景下客户将设备注册到远程服务器中，并管理设备的订阅信息。

5 详细更新内容

5.1 内核

银河麒麟高级服务器操作系统 V11 基于全新的社区 LTS 6.6 内核开发，版本从 v6.6.0 迭代开发至 6.6.0-32.7。银河麒麟高级服务器操作系统 V11 2503 内核集成了多个自研内核特性、特别是对于存储、虚拟化和安全模块等核心模块进行了全方位提升，同时吸收 openEuler 社区、CentOS 社区、上游社区等多个主流内核社区的优秀成果。

除了功能特性，银河麒麟高级服务器操作系统 V11 在生态兼容方面也做了全面适配，包括国内外主流 CPU 平台、整机板卡等。内核累积合入功能特性近 120 项，适配 CPU 平台 17 款，适配板卡 42 款，累计更新 patch 近 30000 个，修复问题数量 570 余个，修复 7 分及以上的高危 CVE 漏洞 773 个。

5.1.1 支持上游内核创新特性

● 内存管理 folio 特性：Linux 内存管理基于 page 转换到由 folio 进行管理，相比 page，folio 可 以由一个或多个 page 组成，采用 struct folio 参数的函数声明它将对整个（1 个或者多个）页面进行操作，而不仅仅是 PAGE_ SIZE 字节，从而移除不必要复合页转换，降低误用 tail page 问题；从内存管理效率上采用 folio 可减少

LRU 链表数量，提升内存回收效率，减少 page fault 次数，一定程度降低内存碎片化。

● EEVDF 调度：EEVDF 全称“Earliest Eligible Virtual Deadline First”，是一种全新的公平调度器，旨在替代使用了十多年的 CFS（Completely Fair Scheduler）。它的核心目标是在保持公平性的基础上，显著改善延迟敏感型任务（如实时任务、交互式任务）的响应性和确定性。具体而言，在保障任务运行时间分配公平的同时，优先在没有满足应得运行时间的任务中，选择任务 deadline 最近的任务，从而保障任务的调度时延，解决了原有的 CFS 调度器只能公平分配任务运行时间，不能满足任务时延要求的问题。

● 可扩展编程调度特性 sched_ext：利用 eBPF 技术，允许动态定义和修改 CPU 调度策略，突破了传统内核调度器的限制。其核心目标是提供极致的可扩展性和灵活性，让开发者能在生产环境之外安全地实验、定制和优化调度行为。其关键特性如下：

■ 用户态编写调度器：在用户态使用 C 语言或者 Rust 语言，编写调度逻辑，使用 GCC 或者 CLANG 编译成字节码。

■ 动态加载与替换：编译后的 eBPF 调度程序可以在系统运行时动态加载到内核，无需重启或重新编译内核，也可随时卸载或替换成另一个调度器。

■ 加载后的 eBPF 调度程序，通过严格的验证器保证其安全，被 eBPF 虚拟机在内核态安全、高效地执行。

● MPTCP 多路径全量特性支持：MPTCP 协议诞生旨在突破传统 TCP 协议的单一路径传输瓶颈，允许应用程序使用多个网络路径进行并行数据传输。这一设计优化了网络硬件资源的利用效率，通过智能地将流量分配至不同传输路径，显著缓解了网络拥塞问题，从而提高数据传输的可靠性和吞吐量。 目前，MPTCP 在下述网络场景中已经展现出了其优秀的性能：

■ 网络通路的选择：在现有的网络通路中，根据延迟、带宽等指标评估，选择最优的通路。

■ 无缝切网：在不同类型网络之间切换时，数据传输不中断。

■ 数据分流：同时使用多个通道传输，对数据包进行分发实现并发传输，增加网络带宽。

● dm vdo 去重和压缩功能特性支持：dm-vdo (Virtual Data Optimizer) 是 Linux 内核设备映射器 Device Mapper 框架提供的一个虚拟块设备驱动，它通过在块存储层透明地实现高级数据缩减功能，显著提升物理存储利用率：其核心依赖于 vdo 内核模块，利用模块中子模块实时计算数据块哈希值进行在线去重，仅存储唯一数据块副本并通过指针引用重复块；同时，对去重后的数据采用高效算法进行异步压缩，将数据打包存入固定大小的物理块中。结合零块消除，它能大幅减少冗余数据、节约存储空间 (尤其在虚拟机、备份等场景效果显著)，且整个过程对上层应用和文件系统完全透明，是高性价比的理想内核级方案。

● bcachefs 文件系统全量特性支持：bcachefs 是一种先进的写时复制 CoW 文件系统，旨在提供企业级存储解决方案；其核心特性包括：数据完整性保障（端到端校验和与自我修复机制）透明加密（AES-256-XTS 文件级加密）与多算法压缩（LZ4/Zstd），支持多设备管理如副本（类 RAID1）和擦除编码（类 RAID5/6）冗余，并具备高级数据功能如 Reflink 克隆（秒级空间高效复制）、可写快照与子卷，项目级配额控制，同时通过混合存储分层（SSD 缓存加速 HDD）实现高性能与高可靠性，适用于数据库虚拟化及大规模存储场景。

5.1.2 自研创新特性

● 新增 kalert 智能故障预警框架：通过统一的内核故障预警框架来解决故障上报的零散性、极端性、易忽略性等，以实现故障上报、故障监测和故障管理的统一性。

● 支持 ketones 内核观察 ebpf 工具集：ketones 是现代化高性能 eBPF 工具包，提供多个监控和可观测性工具，作为 BCC 的简化替代方案，提供增强的内核可观测性能力。

● 支持 netmaster 网络故障定位 ebpf 工具集：

  ■ 网络报文跟踪：跟踪网络报文从网卡进入网络协议栈到释放或丢弃的过程中经流内核中报文处理的相关函数，通过分析报文在内核中经流的相关函数的路径，与报文生命周期，可以快速分析与定位一些网络问题，并且能快速了解一些网络行为。

  ■ 网络故障诊断：通过将内核中一些关键报文处理函数异常信息与日常问题处理相关经验结合形成内核网络协议栈异常知识库，将实际采集到的信息

与知识库进行匹配，以此来快速诊断相关网络故障，并提供一些异常处理建议。

- 网络丢包监测：跟踪内核网络协议栈丢包事件，结合获取到的内核提供的丢包原因，快速了解定位内核丢包原因。

● 优化大页场景下的内存水位线预留：以支持透明大页的使用需求，达到自适应调节预留内存的情况，释放内存给业务端使用。

● 支持 xfs 文件缓存并发写：支持对单个文件的缓存并发写入特性，大幅提升多进程对单文件缓存写入性能。。

● 支持 xfs 全新 AF 空间分配算法：提供一种全新的空间分配算法，增加 xfs 在极度碎片化的情况下的空间利用率。

● 新增 sock 多路转发功能：针对网络转发应用场景，在内核 socket 层直接实现网络报文转发，优化报文转发路径，减少数据拷贝开销，提升网络转发效率，支持传输层协议的转换以及一对多的网络转发模型，满足高并发、低延迟的网络转发需求。

● 新增缓存 IO 亲和功能：在飞腾 S5000C 平台上，优先使用设备所在节点内存，降低跨 die 率，提升 I/O 性能。

5.1.3 其他重要更新

- CPU 型号识别模块
- 飞腾平台 Xor-neon 加速
- 龙芯平台支持 crash kernel=X,[high,low]启动参数
- 龙芯平台支持 kfence 功能
- bonding 多路转发
- igb 驱动 bonding 延时优化
- 网络自适应亲和优化
- IP-SAN 优化
- BFQ 调度器优化

- 虚拟显示驱动
- gpu 固件加载功能
- 飞腾 2000plus 平台温度监控驱动
- 飞腾平台 SUART 驱动
- BMC 在线检测功能
- 硬件与设备驱动过期提示框架
- kabi 检测模块
- 新增 ascii_logo 的商标 LOGO 显示
- 自动化内核模块初始化预防资源泄露
- kvisor 虚机驱动
- 内核校验软件
- Unixbench 性能优化
- ARM 架构 kvm/qemu 虚拟机支持 vcpu 热插拔
- 支持飞腾虚拟机从 2500+热迁移到 S5000C 上
- 支持在 TCP 中使用 fastopen 进行零拷贝
- virtio-iommu 驱动程序
- blk-iocost 功能支持
- 允许在启动和运行时选择内核抢占模型
- 增加了损耗更小的内存检测工具 KFENCE
- 公共的 IOPAGEFault 支持
- SupportforconcurrentTLBflushing
- 突发 CFS 带宽控制器支持
- smb 服务端内核态支持

- 内存访问监控机制 DAMON 支持
- Rust 支持
- 龙芯架构 kvm 虚拟化支持
- ARM 架构 virtcca 支持
- 为 vfio 在热迁移中支持 debugfs
- virtio_pmem 支持 SHMEM_REGION 特性
- vDPA 支持用户层查询 virtio 块设备信息
- virtio 添加了对 no-reset virtio PCI 电源管理的支持
- pkvm 安全虚拟机功能
- largefolio 对 mlock、khugepaged、pagefault 等框架的改造
- 支持 cgroupv2
- 支持 MGLRU 特性
- Thread-basedNAPIpolling 支持
- 新增 TCPAuthenticationOption 功能
- 支持 ARM8.6 特性 TWED
- virtio-net 新增 XDP 特性 NETDEV_XDP_ACT_XSK_ZEROCOPY
- 虚拟设备 mtty 支持迁移 P2P 状态以及脏页记录
- 支持 NUMA 感知的 qspinlock 自旋锁
- 内核热补丁增强
- BPF 支持：
  - 支持 CompileOnceRunEverywhere（CO-RE）技术和 BTF 类型格式
  - 引入 CAP_BPF 权限机制
  - 支持 BPFtrampoline 技术

- 支持 BPFSTRUCT_OPS
- BPF 支持内核函数调用(kfunc)
- 支持获取 bpf_link 详细信息的能力
- 支持动态指针（structbpf_dynptr）
- 新增了类型匹配（typematches）关系
- 支持特定用于 BPF 的内存分配器
- 支持破坏性 bpf_kfuncs（bpf_panic）
- 支持用户自定义 BPF 对象，实现自定义数据结构
- 支持 BPF 开放编码（迭代器），允许在 BPF 程序中实现更少限制的循环
- 支持 arenas 特性，即在 bpf 程序和用户空间共享内存区域
- 支持 netkit 设备，即可以在 L3 或 L2 模式下运行的 BPF 可编程网络设备
- 新增 BPF_PROG_TYPE_FLOW_DISSECTOR、
BPF_PROG_TYPE_CGROUP_SYSCTL、
BPF_PROG_TYPE_RAW_TRACEPOINT_WRITABLE、
BPF_PROG_TYPE_CGROUP_SOCKOPT、BPF_PROG_TYPE_TRACING、
BPF_PROG_TYPE_STRUCT_OPS、BPF_PROG_TYPE_EXT、
BPF_PROG_TYPE_LSM、BPF_PROG_TYPE_SK_LOOKUP、
BPF_PROG_TYPE_SYSCALL、BPF_PROG_TYPE_NETFILTER 等 BPF 程序类型；
- 新增 BPF_MAP_TYPE_QUEUE、BPF_MAP_TYPE_STACK、
BPF_MAP_TYPE_SK_STORAGE、BPF_MAP_TYPE_DEVMAP_HASH、
BPF_MAP_TYPE_STRUCT_OPS、BPF_MAP_TYPE_RINGBUF、
BPF_MAP_TYPE_INODE_STORAGE、BPF_MAP_TYPE_TASK_STORAGE、
BPF_MAP_TYPE_BLOOM_FILTER、BPF_MAP_TYPE_USER_RINGBUF、
BPF_MAP_TYPE_CGRP_STORAGE、BPF_MAP_TYPE_ARENA 等 MAP 类型

5.2 基础组件

5.2.1 anaconda :操作系统安装配置程序

Anaconda 是专为操作系统安装配置的工具。该组件支持键盘、语言支持、时间与日期、安装源、软件分组、安装位置、网络与主机名、账户密码等多样化配置选项，让用户能够根据个人偏好或项目需求对操作系统进行定制。该组件同源支持 x86_64、aarch64、loongarch64 等多种平台。Anaconda 组件具备跨平台兼容性、支持广泛的处理器架构且提供稳定的系统配置功能。

- 优化 DNF 模块安装流程：调整使用多线程操作 DNF 模块安装，删除 Py_Initialize 检查，提高安装软件包的效率，节省用户安装操作系统的时间。

- 增强附加组件集成：附加组件调整为使用 Anaconda DBus 附加组件的方式，确保组件间的无缝协作与高效运行。

- 加固系统安全：在镜像制作中已经固定策略，kickstart 文件不再支持密码策略变更，增强系统安全防线，为用户提供更加稳定的运行环境。

- 灵活 Swap 空间配置：调整存储 swap 空间设置为可选分区策略，增强用户根据需求自由配置硬盘分区的灵活性，实现资源分配的个性化与最优化。

- 优化 Root 用户密码配置界面：对 Root 用户密码界面的布局进行调整，提升界面布局的直观性与易用性，增强用户配置体验的整体友好度。

- 强化代码质量保证：采用 unittest python3 框架进行单元测试，确保软件功能准确无误，同时提升安装程序代码的健壮性与质量，为用户提供稳定高效的安装服务。

5.2.2 grub2 :操作系统引导加载程序

GRUB 2（GRand Unified Bootloader 2）是一个广泛使用的引导加载程序，用于在计算机启动时加载并引导操作系统。作为 GNU 项目的一部分，GRUB 2 是 GRUB 引导加载程序的第二个主要版本，它取代了之前的 GRUB 0.9x 版本（也被称为 GRUB Legacy）。在麒麟 Linux 发行版中，GRUB 2 是默认的引导加载程序。

- 扩展编译器兼容性：新增 GCC 13 与 clang 14 编译标准的支持。

- 引导加载程序接口：初步实现对引导加载程序接口的支持，为系统启动流程增添更多灵活性和定制性。

- UEFI 与 GRUB 动态内存管理：通过 UEFI 接口，动态增加 GRUB 运行时内存支持

- 提升系统启动效率与资源利用率。

- 新增 PCI 和 MMIO UART 支持，增强系统兼容性。

- 新增 SDL2 支持，增强 grub2 兼容性。

- 支持 x86_64/aarch64/loongarch64 平台安全启动。

- 系统稳定性与兼容性提升：对 TPM（可信平台模块）驱动程序进行修复，当遇到未知 TPM 错误时，让系统默认可启动。

- 模块精简：移除不再需要的 efi_netfs.mod、blscfg.mod、version.mod 模块，减少系统冗余，提升效率。

- 特性调整：不再支持 menu_auto_hide 和 menu_show_once 特性，优化代码，提升可维护性。

- 支持可信启动和安全启动功能。

- 修改可信启动配置文件异常重启无法进入系统的问题。

- /etc/default/grub 新增 KYLIN_ROOT_USE_UUID 配置项，配置开启时，可使 grub.cfg 中 root 参数优先使用磁盘 UUID。

- loongarch64 平台，支持加载体积更大的 initramfs，增强 grub2 兼容性。

- 优化兆芯 CPU 在传统模式下的 initramfs 加载速度。

5.2.3 shim :操作系统引导加载程序

Shim 是一款轻量级但功能强大的 UEFI 引导加载器，在增强系统启动安全性方面发挥着重要作用。它通过内置证书验证、TPM 支持和系统协议安装等机制，确保了启动过程的完整性和安全性。

- 默认开启 sbat 防回滚功能。

- 支持 x86_64/aarch64/loongarch64 安全启动。

5.2.4 python-blivet :用于系统存储配置的 python 模块

Python-blivet 是一个专为系统存储配置设计的 Python 模块。它提供了丰富的接口和功能，用于管理和配置系统存储设备，如硬盘、分区等。

- 文件系统在线调整大小支持：支持在线调整挂载状态的文件系统大小，通过 flags.allow_online_fs_resize 控制。

- 存储支持扩展：增加对 NVMe 和 NVMe over Fabrics 设备的识别和支持。支持根据挂载点设置 GPT 分区 GUID。

- 功能裁剪：移除对 DMRAID 设备的支持，由 mdadm 接管 BIOS RAID 设备。移除 DMRaidArrayDevice、flags.noiswmd 和 flags.dmraid。

- 提升性能与灵活性：支持创建和附加 LVM 写入缓存设备，提升存储性能。允许在现有 LVM VDO 卷上启用或禁用压缩与去重。

- 测试套件改进：将测试套件拆分为单元测试和存储测试，提高测试效率和覆盖率。

- 新存储技术集成：集成 Stratis 存储管理，支持创建和管理 Stratis 池及文件系统。增加对 LVM 缓存池的支持，提升数据访问效率。

- 设备管理增强：支持新的 LVM 设备文件，用于更灵活的设备过滤和管理。允许通过 ActionConfigureDevice 操作重命名 LVM 卷组和逻辑卷。

- 设备支持：增加对 NPIV（N_Port ID 虚拟化）启用的 zFCP 设备的支持。

5.2.5 dracut : RAM 磁盘（initramfs 或 initrd）管理工具

dracut 是一个在 Linux 系统中广泛使用的工具，主要用于生成 initramfs（Initial RAM File System，初始内存文件系统）映像文件。Dracut 通过自动检测系统中的硬件设备并将相应的模块添加到 initramfs 中。

- 新增--enhanced-cpio 选项来调用 dracut-cpio 进行更高效的 cpio 归档。

- 新增检查目标内核是否支持 zstd 压缩算法。

- 新增--parallel 选项以支持并发执行。
- 新增 ZFS 探测支持。
- 新增--squash-compressor 选项，用于指定 squash 压缩器。
- 在 dracut-install 中支持处理使用 ZSTD 压缩的.zst 后缀的固件。
- 新增 fido2 模块，支持 FIDO2 认证标准。
- 新增 pcsc 模块，支持 PC/SC 智能卡接口。
- 新增 pkcs11 模块，支持 PKCS#11 加密标准。
- 新增 systemd-integritysetup 模块，用于 systemd 下的完整性保护设置。
- 新增 newc 归档文件制作工具。
- 新增 crosvm 的 rust 参数解析库。
- 新增对 squash 压缩器的支持。
- 新增检查系统根文件系统的 fstab。
- 新增用于网络管理的 connman 支撑模块。
- 新增用于监控 LVM thinpool 的 lvmthinpool-monitor 模块。
- 新增 rd.luks.key.tout 的文档。
- 新增 virtiofs 模块，支持 virtiofs 根文件系统启动。
- 默认安装了 tmpfiles.d 配置文件，用于管理 multipath 设备的配置文件。
- 新增 overlayfs 模块，支持 overlayfs 文件系统。
- 新增加了 efi_secret 驱动，用于 EFI 安全特性。
- 新增 systemd-pcrphase 模块，用于管理 PCR（Platform Configuration Register）。
- 新增 systemd-portabled 模块，支持便携式系统服务。
- 新增 systemd-pstore 模块，用于管理系统 pstore（Platform Storage）。
- 新增 test、test-makeroot、test-root 模块，共享测试用例代码，以提高测试效率

和代码复用性。

● 合入安全模块初始化组件，删除不再使用的模块 kic 和 dac，修复标记初始化失败以及开启三员失败等问题。

● 合入安全模块初始化组件。

● 删除不再使用的模块 kic 和 dac。

● 修复标记初始化失败以及开启三员失败等 bug。

5.2.6 glibc :标准 C 库

glibc 是 GNU 发布的 libc 库，即 c 运行库。glibc 是 linux 系统中最底层的 api，几乎其它任何运行库都会依赖于 glibc。glibc 除了封装 linux 操作系统所提供的系统服务外，它本身也提供了许多其它一些必要功能服务的实现，V11 2503 相比 V10 有以下主要特性。

● malloc 引入了 hugetlb 特性，并支持相应可调整参数的配置，让用户自己按需申请大页来提升特定场景的性能。

● Linux 平台上添加了对 loongarch64 的支持，保证各架构之间的代码同源。Linux 平台上支持了 pidfd 功能，提供了对进程的访问，能帮助服务管理器处理 PID 重用问题。

● 新增函数 arc4random、arc4random_buf 和 arc4random_uniform，提供比 rand/random 高质量的随机数生成。

● 将在 libpthread, libdl, libutil, libanl 库的所有功能已经集成到 libc 中，支持更顺畅的就地升级。

● 引入了 Safe-Linking 机制保护，将堆块头部保存的地址重新计算，主要应用于 tcache 与 fastbins 中，可以防止指针被劫持。

● aarch64 在 rmv8.5-a 和 armv8.3-a 体系结构扩展环境下支持标准分支保护安全加固，为间接分支及其目标提供了控制流完整性(CFI)保护，有助于限制 JOP(Jump Oriented Programming)攻击。

● 在 x86_64 平台基于 glibc-hwcaps 机制，通过 avx2 向量指令优化 strstr 函数，通

过非临时存储技术优化 memset 函数。

- 新增支持 tcache 小内存块动态可调参数 glibc.malloc.tcache_count_dynamic 和线程栈缓存动态可调参数 glibc.pthread.stack_cache_size_dynamic。
- 支持兆芯 KH-40000 处理器硬件架构特性。
- 基于 glibc-hwcaps 机制，通过 AVX2 向量指令、以及非临时存储技术优化 x86_64 架构下 strstr、memset 函数。
- 升级 Unicode 标准至 15.1.0。

5.2.7 openJDK :Java 开发套件

Java Development Kit (JDK)是一套用于开发和运行 Java 应用程序的工具集。它包括了编译器（javac）、运行时环境（Java Runtime Environment，JRE）、类库、文档生成工具（javadoc）、调试工具以及其他开发和测试工具。JDK 提供了所有必要的组件，使开发者能够编写、编译、调试和运行 Java 程序，是 Java 开发的核心工具包。

OpenJDK 8 增强特性：

- 支持识别海光 CPU 平台，优化相关 CPU 特性使能状态。
- 支持兆芯 CPU 平台，优化相关 CPU 特性使能状态。
- 增强在 x86_64 平台上原子操作在虚拟化 CPU 扩容场景下的稳定性。
- C2 编译器支持 x86 AVX512 指令集。

OpenJDK 11 增强特性：

- 支持识别海光 CPU 平台，自动使能相关 CPU 特性。
- 支持识别兆芯 CPU 型号，优化相关 CPU 特性使能状态。

OpenJDK 17 增强特性：

- 优化了核心库中的 TreeMap 操作，新增“-XX:NodeSize”参数调节 Treemap 节点容量。

新引入 OpenJDK 21，包含主要特性：

- 引入虚拟线程，简化并发编程模型，减少线程管理的开销。
- 支持分代 ZGC，性能提升，减少暂停时间。
- 扩展了模式匹配的应用场景，包括 switch 表达式和类型检查等，提高代码的可读性和简洁性。
- 引入字符串模板，简化字符串的使用。
- 提供外部函数和内存访问的 API。

5.2.8 systemd: 系统服务管理组件

systemd 是操作系统中的一个系统和服务管理器，以 PID 1 进程运行。用于初始化系统并管理服务。它为系统启动和管理提供一套完整的解决方案，包括进程服务管理、维护挂载与自动挂载、设备管理、登录和日志等，同时提供了各种管理工具方便维护系统。

- systemd 升级到 v255，同源支持 x86_64/aarch64/loongarch64 等架构。
- 新增僵尸进程回收和进程监控自愈功能，实现回收僵尸进程资源，以及关键进程的监控和自愈恢复，提升系统健壮性和稳定性。
- 新增"systemd-bsod"蓝屏功能，在蓝屏时显示二维码，用于获取导致引导失败的错误的更多信息。
- 新增"systemd-storagetm"组件工具，它开放所有本地块设备作为 NVMe TCP 设备，完全自动。旨在用于安装程序和调试快速访问本地磁盘。
- 新增"systemd-vmspawn"工具，它为虚拟机提供了与 systemd-nspawn 为容器提供的相同的接口和功能。
- 新增"varlinkctl"工具，允许与 Varlink 服务进行接口连接。
- 新增 systemd-measure 工具，systemd-measure 是一种计算和签署期望值的新工具。
- 新增 systemd-pcrphase 工具，systemd-pcrphase 是一个新工具，在调用系统运行时，测量 TPM2 PCR 11 中的附加单词，以标记启动过程的里程碑。

- 新增"systemd repat"工具，可以为 GPT 分区表的幂等声明性来重新分区。

- 添加了一个新组件"userdb"以及客户端工具"userdbctl"，能以 JSON 格式定义丰富的用户和组记录， 对经典的 struct passwd 和 struct group 的扩展结构。

- 添加了一个小型的新服务 system-homed.service，用于通过内置加密安全地管理主目录。完整的用户记录数据与主目录统一， 从而使主目录自然可迁移。

- mkosi 制作 initrd 新增了更多参数控制和优化改进。

- bpf 程序能用 bpf-cc 来进行编译。

- systemd coredump 现在提取 ELF 构建 id 信息,处理 coredump 并将其包含到报告中。此外，查找 ELF.note.package 部分，其中包含关于崩溃进程的发行版软件包的元信息。

- systemd-detect-virt 工具进行优化，新增检测虚拟机类型，支持更多平台；系统 TPM 安全启动模块的改进优化。

- bootctl 新增 2 个子命令 kernel-identify 和 kernel-inspect，kernel-identify 打印内核映像文件的类型，并且 kernel-inspect 提供嵌入式命令行和内核版本的信息，另外 bootctl 目前可以在所有 EFI 系统上生成系统令牌。

- systemd-boot 优化更新和功能增强。

5.2.9 bash: 命令行解释器与脚本语言

Bash (Bourne-Again SHell) 是一款广泛使用的命令行解释器和脚本语言，支持复杂的命令行操作与脚本编程，具备丰富的内置命令、环境变量管理和流程控制结构。它兼容 POSIX 标准，可在多种 Unix-like 操作系统上运行，为用户和系统管理员提供高效、灵活的交互界面与自动化工具。

- 重写命令替换解析代码，提供更完善的语法检查，并更早地捕获错误。

- 内置的 unset 现在尝试将参数视为数组下标，而进行不解析或展开。

- command -p 不再在哈希表中查找指定的命令。

- 支持对 shell 脚本的执行管控。

5.2.10 python3: 高级编程语言

Python3 是一种广泛采用的高级编程语言，以其简洁易读的语法和强大的标准库而著称。它支持面向对象、过程式和函数式编程范式，适用于 Web 开发、数据分析、人工智能等多种应用场景。Python3 提供了丰富的第三方库，能够高效地进行跨平台开发。Python3 版本升级到 3.11，具有以下主要特性:

- 拥有更快的 CPython 解释器，整体性能提升 25%左右。
- 发生异常时，解释器可以精确标注出错误的表达式。
- 新增 tomllib 模块，用于解析 TOML。
- 支持程序能够同时抛出和处理多个不相关的异常。
- 引入了支持可变数量类型参数的 TypeVarTuple。
- 新增类型注解 LiteralString，增强系统安全性。
- 对 asyncio，contextlib，dataclasses，datetime，enum 多个模块进行性能增强和功能改进。
- 新增 PyType_GetName()、PyType_GetQualName()、PyThreadState_EnterTracing()、PyThreadState_LeaveTracing()函数。

5.2.11 coreutils: 基础命令工具集

Coreutils 是一套基础的 Unix 命令行工具集合，包含如 ls、cp、mv、rm 等在内的基本文件和目录操作命令。这些工具遵循 GNU 项目的精神，提供了强大且灵活的功能，支持各种选项和参数，适用于日常系统管理和脚本编程，是 Unix-like 环境中的必备工具。

- comm、cut、join、od 和 uniq 命令会在收到写错误时立即退出，这在读取无界输入时很重要。
- 对 Split 进行了优化，当从 SSD 读取数据时，提高了 5%的吞吐量。
- cp、mv 和 install 命令支持--debug 选项来打印文件被复制的详细信息。
- chsum 接受--raw 选项来输出原始二进制校验和。

- chsum 接受--base64 选项来打印 base64 编码的校验和。

5.2.12 util-Linux: 系统管理工具集

Util-Linux 是一套包含多种实用工具的集合，提供了诸如 mount, umount, fdisk, mkfs, blkid 等命令，用于磁盘分区、文件系统管理和设备挂载等操作。这些工具在 Unix-like 系统中广泛应用，为系统管理员提供了高效便捷的系统管理手段。

- 伪文件系统中新增对 tracefs、vboxsf、virtiofs 的支持。
- 添加对 loongarch64 平台的支持。
- fstrim 命令添加 --types 选项，按文件系统类型过滤。
- 新增 waitpid 命令。
- renice 命令支持 posix 兼容的-n 选项，并添加--relative 选项。
- chfn 和 chsh 命令支持-V 选项。
- blkdiscard 命令新增-q 选项。
- Btr 命令支持 sha256。
- mkfs.cramfs 和 mkfs.bfs 新增支持 BSD 锁。
- 修复了 wall 命令在处理用户名时可能发生的内存泄漏问题。
- 修复了 setpriv 命令中处理 --secbits 参数时的一个内存泄漏和潜在段错误问题。
- 修复了 hwclock 工具中 save_adjtime 函数的内存泄漏问题。
- 修复了 su 工具中在 PAM 错误处理时的释放后使用问题。
- 修复了与 procps-ng-i18n 共同安装时产生的冲突问题。
- 修复了 libmount 处理空值挂载选项、某些挂载标志、挂载点子文件系统迭代顺序的逻辑错误问题；特定错误处理路径中潜在的内存泄露问题；remount 操作中多个 atime 选项的互斥性问题。
- 修复了 sfdisk 因翻译文件错误导致的可能崩溃问题。

5.2.13 golang：Go 编程语言开发工具

golang 是一个包含 Go 语言编译器、标准库、依赖库及开发环境支持的开源开发工具，支持跨多种操作系统和架构编译，支持交叉编译，内置标准库涵盖从基本数据类型到网络通信、并发编程、加解密等多个领域，为开发者提供强大的开发环境和工具，支持快速、高效地开发各类 Go 应用程序。Go 版本升级到 1.21，具有以下主要特性：

- 支持 loongarch64 平台。
- 默认启用 Go Modules 特性。
- 提高垃圾收集器工作效率，降低应用尾部延迟及内存使用量。
- 引入 Soft memory limit 触发策略，使内存回收触发收益更高，性能影响更小。
- 支持 x86_64 和 aarch64 等架构实现了使用寄存器而非堆栈传递函数参数和结果的方法。
- 支持泛型的编译器的类型检查程序。
- 引入 PGO 特性进行编译器/链接器优化。
- 改进兼容性、加强代码规范检查，明确依赖包初始化顺序的算法，增强对泛型的类型推断能力。
- 支持 loongarch64 平台对 plugin 插件编译模式、动态库生成和加载。

5.2.14 rsyslog：系统日志处理工具

rsyslog 是一种快速的系统日志处理工具，能够处理各种来源的大量日志消息，采用模块化设计支持灵活扩展和配置，支持对日志消息进行复杂的转换和处理，如过滤、格式化、增强、聚合等操作，使得日志数据更易于管理和分析，并能将处理后的结果输出到多种不同的目的地，如本地文件、远程服务器、数据库等，适用于大多数需要高效日志管理的系统和应用场景。

- 新增输出模块 omazureeventhubs，用于将日志数据快速可靠地发送到 Microsoft Azure Event Hubs。在 omazureeventhubs 模块中修正了对传输关闭失败的处理，提高了稳定性和可靠性。

- 改进了 imjournal 模块，现在支持多个输入。
- 在 imkmsg 模块中增加了新的参数，可以修改读取模式和内核时间戳解析。
- 修复了在现代 systemd 系统上启动时的问题，现在使用 /proc 文件系统获取文件句柄以便在启动时关闭。
- 修复了 TLS 子系统在启动时发现的小内存泄漏问题，进一步提升了系统的健壮性。
- 新增当目标文件是/dev/null 时，跳过所有实际的 omfile 操作的特性。
- 修复了 imtcp 和 omfwd 模块无法识别 StreamDriver.CRLFile 参数的问题。
- 修复了 omazureeventhubs 模块在处理 PN_DELIVERY 事件时的内存泄漏问题。

5.2.15 openSSL：SSL 和 TLS 协议实现库

openssl 是一个功能强大的加密库，提供了 SSL 和 TLS 协议的开源实现，同时也支持多种加密算法和工具，广泛应用于互联网安全传输。openSSL 版本升级到 3.0.12。

- 增加了对 Kernel TLS (KTLS) 的支持，显著提升了内核级别的 TLS 性能。
- 增加了生成非对称密钥对的便捷函数，以及新的编码和解码 API (OSSL_ENCODER 和 OSSL_DECODER)。
- 增加了对现代加密算法（如 X25519、X448、Ed25519、Ed448、SHAKE128 和 SHAKE256）的支持，并将其包含在 FIPS 提供程序中。
- 实现了证书管理协议（CMP）和一个功能全面的 HTTP 客户端，增强了客户端和服务器的证书管理和网络交互功能。
- 增加了 openssl mac 和 openssl kdf 命令，利用新的 EVP_MAC 和 EVP_KDF API 提供多种 MAC 和 KDF 支持。
- 增强了 openssl list 命令，增加了许多新选项。
- 增加了迁移指南和对完全可插拔的 TLSv1.3 群组支持。
- 弃用了多种低级别加密和摘要函数，包括 MD2、MD4、MD5、MDC2、RIPEMD160、SHA1 等摘要函数，以及 AES、Blowfish、Camellia、CAST、DES、IDEA、

RC2、RC4、RC5 和 SEED 加密函数。

- 弃用了 OCSP_REQ_CTX、EC_KEY、RSA、DSA、DH 及其相关方法。
- 弃用了 ENGINE API，并引入了新的提供程序概念，作为 ENGINE API 的替代方案。
- 移除了 DTLS 特性中的心跳消息。
- 弃用了 RAND_DRBG API 以及一些 ERR_load_ 函数。
- 修复了多个安全漏洞，增强了系统的安全性和稳定性，包括缓冲区溢出、空指针解引用、定时攻击等问题。
- 增强了对硬件架构的支持，优化了多种算法的性能，显著提升了整体运行效率。
- 改进了证书验证和加密密钥处理，提升了系统的安全防护能力。
- 支持麒麟证书。
- 修复 ec 生成公钥失败。
- 修复使用国密生成私钥后加密私钥失败。
- 增加生成 ec 私钥证书时可以设置口令。
- 支持兆芯 CPU 国密算法。
- 支持 TLCP 协议。
- 支持 ZUC 祖冲之算法。
- 支持 DRBG SM3 算法支持，满足 GM/T 0105-2021 标准。
- 支持 TLS 1.3 协议国密支持，满足 RFC8998 标准。
- 解决在 TLCP 协议时导出密钥 material 的失败问题。
- 解决兆芯 sm2 运算时出现的段错误问题。
- 添加 SP 安全编译参数-fstack-protector-all，提升安全检查等级。
- 通过这些改进和优化，OpenSSL 3.0.12 不仅在功能上有大幅增强，还显著增强了

● 统的安全性和稳定性，满足了现代互联网应用对高效、安全的加密库的需求。

5.2.16 openSSH: SSH 协议实现库

Openssh 是一个功能强大的 SSH 协议实现库，提供了包括 SFTP 客户端和服务器在内的全面支持，广泛应用于安全数据传输。OpenSSH 版本升级到 9.6p1。

● 新增通道闲置超时功能，通过 ChannelTimeout 和 UnusedConnectionTimeout 指令，允许自动关闭在配置时间内未见流量的通道，优化资源管理。

● ssh-keygen 和 ssh-keyscan 命令增加了 -Ohashalg=sha1|sha256 选项，用户可选择输出 SSHFP 指纹的算法，增强了灵活性和兼容性。

● sshd 新增 -G 选项，可在不加载私钥的情况下解析并打印有效配置，便于非特权用户在不生成密钥的情况下评估和验证配置。

● 增加日志详细度，通过 LogVerbose 指令，使用户根据文件、函数和行号模式列表强制最大调试日志记录，提升调试能力。

● 增强对 WebAuthn 签名验证的支持，提高与现代 Web 认证标准的兼容性。

● 默认拒绝远程客户端加载 PKCS#11 模块的请求，可通过 -Oallow-remote-pkcs11 标志恢复之前的行为，提升了安全性。

● 改进 FIDO 支持，增强了对每次使用都需要 PIN 验证的 FIDO 密钥的支持，提供更高的安全性。

● 默认使用混合 Streamlined NTRU Prime + X25519 密钥交换方法，提高对未来量子计算攻击的抗性。

● 通过 UpdateHostkeys 选项，自动迁移到更好的算法，提升密钥管理的安全性。修复 ssh-add 智能卡密钥添加约束的问题，提升了安全性。

● 改进日志记录和错误处理机制，增强了调试和问题排查的效率。

● 通过改进缓冲区管理和数据读取方式，提升了整体性能。

● 支持 UKEY 双因子远程登录认证。

● 新增国密切换命令工具。

- 解决国密主密钥自动生成问题和 ssh-keyscan 扫描主密钥问题。

- 新增通过 PKCS#11 接口使用 SM2 国密算法的能力，进一步提升了保密性和安全性。

5.2.17 audit：Linux 审计框架

audit 是一个用于跟踪和记录系统活动的安全审计框架，广泛用于 Linux 系统的安全监控和合规性检查。audit 版本升级到 3.1.2。

- 更新了用于 Linux 内核的查找表，增强了与新内核版本的兼容性。

- 增加了若干新的 Python 函数，并修改了 Python 绑定，修复了由于 SWIG bug 导致无法从 Python API 设置审计规则的问题，不再需要任何变通方法。

- 在 auditctl 中新增了更友好的信号关键字，提升了用户体验。

- 在 ausearch 中增加了对 URINGOP 和 DM_CTRL 记录的解析能力，增强了日志分析功能。

- 强化了 auparse 的功能，更好地处理损坏的日志，提升了日志处理的可靠性。

- 将 audispd af_unix 插件移至独立程序，提高了模块化和可维护性。

- 新增记录类型，增加了对 io_uring 的支持，并支持新的 FANOTIFY 记录字段，提升了审计系统的灵活性和功能性。

- 支持符号表跨版本兼容 V10SP3 2403 版本。

- 支持 kysec_AVC 日志类型。

- 支持 KSAF 相关日志类型。

5.2.18 shadow：Linux 系统账户和认证管理工具

Shadow 是一个广泛应用于 Linux 系统的用户和组管理工具包，提供了创建、修改和删除用户及其属性的功能。shadow 升级到版本 4.14-3。

- 在 useradd 中增加设置 SELinux 标签的功能，并检查 SELinux 是否启用了多级安全 (MLS) 模式。

- useradd 增加了 -F 选项，增强了用户和组管理的灵活性。
- usermod 中添加了 -rG 选项，用于删除特定组。
- 增加了对 lastlog 功能的条件编译支持，以便在不同系统中灵活使用。
- 合并 libshadow 和 libmisc 库，简化了库管理并解决了链接器问题。
- 修复了多个内存泄漏和潜在的 TOCTTOU 问题。
- 支持系统全生命周期的 UID 唯一性检查。

5.2.19 jemalloc :内存分配器

jemalloc 是一个高性能、开源的内存分配器，由 Jason Evans 在 FreeBSD 项目中引入，并经过不断发展，现已广泛应用于各种系统和应用中，包括 Firefox、Redis、Rust、Netty 等。jemalloc 的设计目标是优化多线程环境下的内存分配效率，减少内存碎片，并提高内存利用率。

- 增加大页分配场景下 slab 分配时内存对齐参数的优化 ,减少了内存碎片的产生,提升内存利用率。

5.2.20 rpm :包管理

RPM Package Manager(RPM)是一个强大的命令行驱动的软件包管理工具，用来安装、卸载、校验、查询和更新 Linux 系统上的软件包。RPM 版本升级至 4.18.2 主要更新集中在改进安全性和增强功能性上。

- 改进了 OpenPGP 解析器的安全性，修复了一些潜在的安全问题。
- 更强大和更安全的--restore 功能，用于恢复文件权限等元数据。
- 引入了一个新的交互式 shell，用于处理嵌入式宏和嵌入式 Lua 脚本。
- 添加了 rpmuncompress CLI 工具，简化了解压多个源文件的过程。
- 合入软件包安装、卸载控制检查；软件包安装/升级时更新 Kysec 标记。

5.2.21 dnf :包管理器

DNF 包管理器是下一代 RPM 软件包管理器，旨在解决 YUM 的一些性能和内存使

用问题，同时提供更高效的依赖关系解析和软件包管理功能。DNF 版本升级至 4.16.2 主要更新集中在性能优化、功能改进和用户体验增强。

● 缓存机制改进：新版本通过优化缓存机制，提高了软件包的检索和安装速度。在处理大量软件包时，这种优化可以显著减少等待时间，提高系统的整体性能。

● 依赖关系解析增强：DNF 4.16 版本改进了依赖关系的解析算法，使得在安装和更新软件包时，可以更高效地计算和解决依赖问题，从而确保系统的稳定运行。

● 本地仓库支持：新增对本地仓库的支持，允许用户在没有网络连接的情况下，从本地存储库更新软件包，这为离线更新提供了便利。

● 安全补丁显示：引入 dnf updateinfo list security 命令，可以显示可用的安全补丁，而无需立即安装它们，使管理员可以先评估再决定是否应用这些补丁。

● 命令行界面(CLI)改进：DNF 4.16 版本改进了 CLI，提供了更多友好的错误信息和操作建议，帮助用户更有效地使用 DNF。

● 配置文件简化：新版本简化了 DNF 的配置文件，使得用户可以更容易地设置和管理软件源，进一步降低了使用复杂性。

● 软件包排除功能：新版本增加了--exclude 选项，允许用户在更新时排除特定软件包，这在处理内核更新等敏感操作时非常有用。

● 历史与缓存管理：dnf history 和 dnf clean all 等命令允许用户审查 DNF 操作的历史记录和管理缓存数据，增强了对软件包管理的跟踪能力。

● API 接口扩展：DNF 4.16 版本扩展了其 API 接口，方便开发者和其他管理系统调用 DNF 的功能，提高了其灵活性和可扩展性。

● 多版本 Linux 发行版支持：新版本进一步优化了对多版本 Linux 发行版的支持，确保了在不同环境下的稳定运行。

● 新增安全补丁批量显示和修复：引入 dnf updateinfo list --start-date <YYYY-MM-DD> --end-date <YYYY-MM-DD> 显示特定时间范围内的安全补丁和 dnf upgrade --start-date <YYYY-MM-DD> --end-date <YYYY-MM-DD>来指定修复特定时间范围内的安全漏洞。

- 新增兼容性检查：dnf remove/downgrade/upgrade 等命令支持--compcheck，启用兼容性检查，对于受保护的组件被影响时，提示兼容性破坏警告，需要用户额外二次确认后再完成事务。

5.2.22 postgresql：关系型数据库

PostgreSQL 是一个功能强大、源代码开放的 C/S 关系型数据库管理系统。它支持几乎所有的 SQL 标准，并且提供了许多其他现代数据库系统所没有的高级功能，如复杂查询、外键、触发器、视图、事务完整性、多版本并发控制等。PostgreSQL 以其可靠性、数据完整性、强大的功能集和可扩展性而闻名，适用于从小型个人项目到大型商业应用的各种场景。同步上游社区，PostgreSQL 升级到 15.12 版本。主要包括如下特性增强：

- 防止在关系截断期间启动检查点，避免操作系统崩溃后引发的数据损坏风险。
- 允许数据表的大小超过 1GB。
- 在内存和磁盘排序上进行了性能增强。
- 改进 libpq 引用函数，修复其未遵循字符串长度参数的问题。
- 修复窗口聚合中可能重复使用过时结果的问题。
- 修复系统目录同时进行清理操作与更新操作时，可能出现的目录损坏问题。
- 修复关系截断失败时的数据损坏问题。

5.2.23 gnupg2：免费的 PGP 替代

Gnupg2（GNU Privacy Guard 2）是一个免费、开源、完整且强大的实现，用于遵循 OpenPGP 标准（RFC 4880） 和 S/MIME 标准（RFC 2311 等） 进行加密和签名。它是著名的商业软件 PGP（Pretty Good Privacy）的开源替代品。

- 支持 SM2 签名算法和 SM3 哈希算法。
- 使用 gpgtar 替换 gpg-zip。
- 现在--no-literal 可以和-c/--store 一同使用。

5.2.24 kexec-tools：内核转储工具

内核 kdump 用户态组件，在正常或紧急重启时使用内核的 kexec 特性引导新内核。

- 同源支持 x86_64/aarch64/loongarch64 架构支持。
- 修复 loongarch64 架构 kdump 服务无法启动问题。
- 修复"grep: warning: stray \ before -"问题。
- 添加对无锁环缓冲区的支持。
- 修复 LoongArch64 架构 crash 解析 vmcore 报错问题。
- 修复 LoongArch64 架构部分机型触发崩溃未生成 vmcore 文件问题。

5.3 虚拟化

5.3.1 qemu：软硬件虚拟化模拟器

QEMU（Quick EMUlator）是一个开源的仿真器和虚拟机管理程序。它能够实现对多种硬件平台的模拟，并且可以在不同的操作系统上运行，提供虚拟化支持。QEMU 的主要特点和功能包括：全系统仿真、用户模式仿真、设备仿真、快照和检查点等等。它通常与 libvirt 和其他虚拟化管理工具结合使用，以提供更好的虚拟机管理和自动化功能。它广泛应用于开发、测试和生产环境，支持多种操作系统和硬件架构。V11 2503 同步上游社区升级至 8.2 版本。新增特性主要有：

- 支持 virtio 设备使用 virtio-mmio 总线。
- 支持跨 HostOS 虚拟机热迁移，如从 CentOS 7/8、OpenEuler 热迁移至 V11 2503。
- 支持 aarch64 架构虚拟机 CPU 热插拔功能，提高虚拟机资源分配灵活性。
- 支持飞腾不同 CPU 型号间虚拟机热迁移。
- 支持海光平台 CSV 加密虚拟机功能。
- 支持鲲鹏 virtcca 机密计算虚拟机。
- 支持虚拟化模块独立化，实现块存储模块化，可按需加载。

- 引入 virtio-mem 支持，允许动态、精细地调整 guest 内存大小。
- NVMe 设备模拟 显著增强，支持更多现代特性。
- vhost-vdpa 支持，用于高效硬件加速 virtio 设备。
- vhost-user 协议扩展，支持更多设备类型和特性。
- 增强 AMD SEV (Secure Encrypted Virtualization) 支持。
- 支持 Armv8.5-MemTag (MTE) 内存标签扩展。
- 增强对度量启动 (Measured Boot) 和 TPM (v1.2/v2.0) 仿真的支持。
- 支持 Arm Scalable Vector Extension (SVE)。
- 支持 Armv9 CPU (如 Cortex-X2, A710)。
- 支持 RISC-V Vector (V) Extension v1.0。
- 改进 Hygon Dhyana CPU 支持。
- 新增对 LoongArch 架构的初始支持。
- virtio-blk 支持多队列 (num-queues)。
- 支持 USB Attached SCSI (UAS) 设备。
- virtio-gpu 增强，支持更多 blob 资源类型和上下文初始化。
- 支持 USB4 / Thunderbolt 3 控制器, USB 重定向 (usb-redir) 改进。
- 引入 virtio-sound 设备支持。
- vhost-vdpa 设备支持热迁移。

5.3.2 libvirt：虚拟机管理工具

Libvirt 是一个开源的 API、守护进程和管理工具，用于管理平台虚拟化。它提供了一种一致的方式来管理不同的虚拟化管理程序，包括：QEMU/KVM, Xen, Hypeer-V, VMWare ESX, LXC, OpenVZ 等。它抽象了底层管理程序的复杂性，提供了一个统一的虚拟化管理接口。这包括启动、停止和迁移虚拟机、管理存储和网络接口以及监控资源使用等功能，V11 2503 同步上游社区升级到 9.10.0 版本，新增特性主要有：

- 更换编译系统为 Meson，提升编译速度。
- 支持更多的处理器型号 loongarch64、phytium S5000c 等。
- 支持 aarch64 架构下虚拟机使用 host-model 启动。
- 支持虚拟机内存零拷贝热迁移。
- 支持 virtio-mem 内存热调整。
- 支持 vdpa 网络设备，支持 vdpa 设备热迁移、热插拔。
- 支持热迁移使用 zstd 或 zlib 压缩并行迁移。
- 支持虚拟机外部快照删除，完善外部快照管理功能。
- 支持热迁移 Post-copy 模式失败后恢复虚拟机。
- 引入虚拟机对绝对时钟偏移(Absolute clock offset)。
- 支持 virtio-iommu 在 Q35 以及 aarch64 架构虚拟机中使用。
- 增加虚拟机内存分配线程，启动虚拟机时可指示 Qemu 并行分配虚拟机内存。
- 支持虚拟机脏页计算模式选项，如 page-sampling, dirty-bitmap, dirty-ring。
- 允许通过 Unix 套接字进行热迁移。
- 强化 virtqemud 守护进程，隔离 QEMU 驱动，减少攻击面。
- 默认启用 SELinux/AppArmor 限制，严格管控虚拟机资源访问。
- 深度集成 cgroups v2，支持资源限制（CPU/内存/I/O）的统一管理。
- 引入 virsh domstart --paused，允许虚拟机启动后直接进入暂停状态。
- 支持 virtiofs 文件系统 的热插拔。
- 优化 外部磁盘快照 性能，减少 I/O 阻塞。
- 支持 virtio-gpu 的 Blob 资源。
- 优化 macvtap 设备热迁移兼容性。
- 增强 ARM SVE/SVE2 向量扩展配置。

- 完善 RISC-V 虚拟化。
- 支持 TPM 2.0 持久化存储，增强机密计算（如 SEV、TDX）的集成管理。
- 改进 NUMA 绑定策略，支持更细粒度的 CPU 和内存拓扑配置。

5.3.3 virt-Manager：虚拟机管理器

Virt-manager（Virtual Machine Manager）是一个基于桌面的用户界面工具，用于管理虚拟机。它利用 libvirt 库，支持 QEMU/KVM、Xen 和其他虚拟化技术。通过 virt-manager，用户可以方便地创建、配置、管理和监控虚拟机，并支持快照、资源分配和性能监控等功能。其直观的界面使得虚拟化管理变得更加简单和高效。V11 2503 同步上游社区升级到 4.1.0 版本，新增特性主要有：

- 优化 UI 界面。
- 新增快照树形视图。
- 新增 PCIe 设备热插拔 操作入口。
- VNC/Spice 控制台支持缩放比例锁定。
- 图形化 CPU 拓扑编辑器。
- 支持云镜像自动配置。
- 简化 LUKS 加密磁盘 配置流程。
- 增加 virt-install 等命令的选项配置。
- 支持 aarch64 虚拟机默认添加图形设备。
- 增加银河麒麟高级服务器操作系统发行版本支持。
- 支持网络安装模式自动识别。

5.3.4 edk2：跨平台 UEFI 固件开发环境

EDK2（EFI Development Kit 2）是一个开源的固件开发框架，用于创建基于 UEFI（统一可扩展固件接口）规范的固件。作为 TianoCore 项目的一部分，旨在提供一个模块化和可扩展的固件开发环境。EDK2 支持多种平台和架构，为开发人员提供了丰

富的库和工具，以便在现代计算设备上实现和定制固件解决方案。V11 2503 同步上游社区升级到 202308 版本，新增特性主要有:

- 支持 AMD SEV-ES。
- 引入 TDVF，支持 TD 启动、度量验证、QEMU/KVM 集成。
- 统一内存加密接口 TdxDxe/SevDxe。
- 增强 Measured Boot：兼容 TPM 2.0 PTP 规范，支持 DRTM。
- 添加 vDPA (Virtual Data Path Acceleration) 初始化支持。
- 扩展 EFI Shell：支持 touch、hexedit、dmpstore -b。
- 添加 Cloud Hypervisor 专用构建选项。
- 兼容 microvm 轻量平台。
- 支持 aarch64 架构使用 SATA 虚拟磁盘。
- 同源支持龙芯架构。
- 支持海光平台 CSV 各型号加密虚拟机启动和运行。
- 支持 OpenSSL 3.0。

5.3.5 libguestfs：虚拟机镜像管理工具

Libguestfs 是一个用于访问和修改虚拟机磁盘镜像的开源工具和库。它支持广泛的文件系统和磁盘格式，允许用户在虚拟机关闭状态下执行操作，如查看、编辑、备份、恢复和迁移文件。Libguestfs 提供了多种编程语言接口，以及命令行工具 guestfish，方便用户进行自动化脚本编写和磁盘镜像管理。V11 2503 同步上游社区升级到 1.49.5 版本，新增特性主要有:

- 拆分 virt-v2v、virt-p2v、virt-builder、virt-cat 等冗余工具，使 libguestfs 更容易构建和管理，并专注于 API 功能。
- 删除一些实验性的、不安全的功能，例如 libguestfs live 和 guestfs_add_driver 设备热插拔，提高软件的安全性和易用性。

- 支持使用 qemu/libvirt 特性-cpu max 来选择运行该设备的最佳 CPU。这应该会提高加密磁盘等设备的性能。
- 支持识别银河麒麟高级服务器操作系统 guest，增强功能适用场景。
- 解决无法识别使用 rpm 包管理软件的 guest 的问题，提高软件兼容性。

5.3.6 cloud-hypervisor：轻量化虚拟化 hypervisor

cloud-hypervisor 是一个开源的虚拟机监控器，运行在物理机的 KVM 管理程序之上，旨在为云环境和容器化应用提供高性能、低开销的支持。作为虚拟机监控器，它允许在一个物理机上同时运行多个虚拟机，并提供对这些虚拟机的管理和控制能力。V11 2503 同步上游社区升级到 37.1 版本，新增特性主要有:

- 支持 x86 和 aarch64 架构。
- 支持虚拟机生命周期管理。
- 支持快照创建与恢复。
- 支持 pci 设备以及设备直通。
- 支持 cpu 热插拔，cpu 热插拔仅支持 x86 架构。
- 支持内存热插拔，内存热插拔支持 ACPI 和 virtio-mem 两种方法。
- 支持磁盘热插拔。
- 支持网卡热插拔。
- 支持本地热迁移。
- 支持半虚拟化设备。

5.3.7 kata-containers：安全容器

Kata Containers 是一款专注于安全与性能的高性能容器解决方案，融合轻量级虚拟机技术，基于 OCI 标准，兼具容器敏捷与虚拟机隔离优势。它以独立轻量级虚拟机作隔离空间，杜绝容器间恶意访问，保障数据安全；通过硬件加速与内核优化，实现毫秒级启动，解决性能瓶颈。同时，其能无缝集成 Kubernetes、Containerd 等工具，

便于云原生环境下的应用部署与运维。这种创新融合打破“安全”与“效率”矛盾，是高安全场景下的理想容器选择。银河麒麟高级服务器操作系统 V11 2503 支持 3.2 版本，主要有以下特性：

- 支持极速启动与低开销。
- 支持零侵入式部署。
- 支持独立内核与硬件虚拟化，阻断容器逃逸攻击路径。
- 支持运行时主动防御，确保仅可信镜像可运行。
- 支持多种 Hypervisor(qemu/stratovirt)，适配 x86、arm64 架构。
- 支持灵活配置与动态调整资源，满足不同业务场景的差异化资源需求。
- 支持与 Kubernetes、Docker 等主流容器生态工具无缝适配，管理容器全生命周期。

5.4 容器

5.4.1 containerd：容器运行时

Containerd 是一个简单、稳定和符合 OCI 标准的容器运行时，其用于提供运行容器所需的核心功能。它旨在作为容器化生态系统的构建块，支持多种容器技术。Containerd 专注于提供高性能的容器运行时，减少了资源消耗和提高了启动速度。并具有可扩展性，通过插件系统，允许集成额外的功能和服务，如日志记录、度量和网络策略等。银河麒麟高级服务器操作系统 V11 2503 中引入 1.7.23 版本，主要功能除配合 docker-ce 完成主要容器管理能力外，还包含如下特性：

- 启用了 CRI（容器运行时接口），允许 Kubernetes 更高效地管理容器生命周期。
- 支持 cgroups blockio 控制器。
- 增加了对在容器中注入 CDI 设备的支持。
- 更新了 seccomp 配置文件，以适配自 Linux 5.16 以来新增的系统调用。
- 解决了并发处理管道通信时，createStream 方法直接操作了 sendLock 和

streamLock，可能导致的死锁问题。

- 修复了某些情况下挂载顺序不符合预期的问题。
- 修复了 NRI 中空的 cri 引用导致程序崩溃的问题。
- 修复了对内存和交换内存限制文件的处理，修复了对 memory.memsw.limit_in_bytes 文件不存在时的错误处理。
- 修复了并发写入容器统计信息的问题，解决了 UpdateContainerStats 中的并发写入问题，提高了容器运行时的稳定性。
- 修复了 THP（透明大页支持）补丁添加了对 longarch64 架构的支持，修复了 loongarch64 构建错误，并纠正了日期错误。
- 允许代理插件声明自己的 capabilities,containerd 可以根据插件的能力进行更智能的调度和调用。
- 修复当客户端重试操作时，可能导致多个线程同时访问快照数据，从而引发竞态条件问题
- 修复了一个关于容器资源统计（如 CPU 使用时间）的问题：某些情况下，累计型指标会异常减少，导致监控系统误判。
- 修复 init 进程退出状态丢失的问题
- 修复当某个任务的进程 ID（PID）为 0 时，调用 DeleteTask 并设置 WithForce 参数会失败问题
- 修复 containerd 启动时创建 /run/containerd 目录时权限设置不正确问题
- 修复了在调用 ListPodSandboxStats 接口时可能出现的 ttrpc 连接关闭问题，防止出现 panic 或服务中断
- 改进了当 Shim 层崩溃或异常退出时，PodSandboxStatus 的返回信息，使其更具可读性和可用性
- 增加了对可继承能力（Inheritable Capabilities） 的支持，允许在容器启动时显式地丢弃某些继承自父进程的能力。

- 修复了在 NRI 中由于空指针导致的 panic 问题

- 修复了在使用 ttrpc 协议时的死锁问题：当向管道写入数据阻塞时，可能导致整个服务挂起

5.4.2 runc：低级容器运行时

runc 是一个轻量级的命令行工具，用于运行基于 Open Container Initiative (OCI) 标准的容器。它由 Docker 社区开发，是一个独立的开源项目。作为容器运行时的一部分，runc 提供了直接与底层操作系统交互的能力，是许多容器管理工具（如 Docker、containerd 和 CRI-O）的核心组件。

- runc 升级到 1.1.12 版本，支持对 hugetlb.<pagesize>.rsvd 限制和计数。之前的非 rsvd 版本的 max/limit_in_bytes 并未统计保留的巨页内存。

- 支持在使用 cgroup v2 时通过 memory.peak 和 memory.swap.peak 来读取 max_usage_in_bytes，通过这些信息来追踪容器中的最大内存使用量。

5.4.3 rubik：在离线混部工具

rubik 是一款容器场景下在离线混部工具，可以针对在线业务和离线业务合理分配资源，提高资源的整体利用率。银河麒麟高级服务器操作系统 V11 2503 采用 2.0.1 版本，重点支持以下功能：

- 支持网络 qos 管控功能：使用 oncn-bwm 工具，设置带宽水位线和限制离线业务带宽范围，当在线业务带宽低于或等于水位线时，离线业务允许使用设置的最高带宽，当在线业务带宽高于水位线时，离线任务允许使用设置的最低带宽。有效保证了在线业务的网络吞吐能力。

- 支持海光 4 号 RDT 功能：通过海光 4 号 RDT 功能，控制离线任务的内存带宽和 L3 缓存使用量，优先保证在线业务的内存带宽和 L3 使用量。

- 支持 crio 的 NRI 插件：使用 nri(Node Resource Interface，即节点资源接口。是 containerd 中位于 CRI 插件中的一种扩展机制。NRI 可以提供容器不同生命周期事件的接口，用户在不修改容器运行时源代码的情况下添加自定义逻辑)作为 rubik 的通知机制，当 nri 检测 pod 或者 container 资源进行创建或删除等动作时，rubik 作为 nri

插件自动触发相关事件的处理，摆脱对 apiserver 的依赖，降低 apiserver 的压力。

- 支持 systemd 和 cgroupfs 的 cgroupdriver：rubik 支持不同 cgroup driver、支持不同容器运行时的 k8s 环境。支持 cgroupdriver 和 container runtime 的不同组合。使用场景更加灵活。

- 基于 intel 3 代以上 CPU 的功耗管理特性：rubik 通过为在线和离线业务分配不同工作频率的 cpu，并动态调整，达到节约整机功耗的目的。

5.4.4 ktib：麒麟可信镜像构建工具

KTIB（Kylin Trust Image Builder）是一个包含静态合规扫描、镜像构建、镜像管理等组件的自研开源镜像构建工具，为用户提供了全方位的镜像构建解决方案，帮助用户确保镜像的安全性和合规性。银河麒麟高级服务器操作系统 V11 2503 支持 0.3.0 版本，KTIB 主要包含以下特性:

- 快速构建容器镜像 rootfs 文件系统：KTIB 支持自定义构建容器镜像 rootfs 文件系统；用户可以通过配置文件轻松地定制和扩展 rootfs，满足不同的业务需求。

- 静态合规扫描:支持在构建镜像前对 Dockerfile 进行静态合规扫描；提供默认的扫描策略文件，策略基于 CIS 规范制定；策略文件支持自定义，用户可以根据独立需求，按照官方文档修改策略文件内容，自定义扫描项；支持输出 JSON 格式的扫描报告和相应的修改建议。

- 镜像构建：KTIB 支持基于 dockerfile 构建容器镜像，并且支持所有 dockerfile 指令。

- 镜像管理：KTIB 支持命令行管理镜像，目前提供推送、拉取、列表、删除、登录、镜像持久化保存和多架构镜像 manifest 管理等命令；KTIB 解决镜像构建过程中的安全性和合规性问题，帮助用户构建安全、合规的镜像，并提供了方便的容器镜像管理功能。

5.4.5 NestOS Kubernetes Deployer：Kubernetes 集群部署工具

NestOS Kubernetes Deployer（NKD）是麒麟软件自主研发的 Kubernetes 集群自动化部署工具，具备跨平台支持和多容器运行时兼容能力，适配 libvirt、OpenStack、裸

金属等主流基础设施。NKD 通过参数化配置实现了集群的弹性定制，有效降低了云原生基础设施的运维复杂度，将传统复杂的 Kubernetes 部署过程简化为标准化作业流程，为用户提供安全、可靠、稳定的集群运行环境。银河麒麟高级服务器操作系统 V11 2503 支持 0.3.0 版本，主要有以下特性：

- 多架构兼容：NKD 兼容 x86_64（Intel/AMD）、aarch64（飞腾/鲲鹏）及 loongarch64 架构，确保无论是国产化芯片还是国际主流 CPU 平台，均可实现一致的 Kubernetes 集群部署体验，满足不同硬件环境下的业务需求。

- 多场景支持：NKD 支持虚拟化（如 libvirt、OpenStack）和裸金属部署，兼顾灵活性与高性能。虚拟化部署依托动态资源调度能力，能快速创建/销毁节点，完美支撑 CI/CD 流水线、开发测试等弹性需求；裸金属部署通过 PXE 自动化交付物理机全量算力，避免虚拟化开销，为 HPC、AI 训练、金融低延时等场景提供稳定的运行环境。

- 多容器运行时支持：NKD 支持 docker、containerd、crio 等主流容器运行时，通过标准接口对不同运行时提供统一管理能力，用户可依据安全性、性能及管理需求灵活选用不同运行时。

- 自动化配置管理：NKD 可自动生成 Ignition、cloud-init 或 kickstart 等系统引导配置，并通过预置的 libvirt、OpenStack 及 PXE 模板实现基础设施即代码（IaC），大幅降低人工配置复杂度，实现一键式交付。

5.5 AI：人工智能融入操作系统

智能时代，操作系统的发展必然与 AI 技术深度融合。一方面，将 AI 融入操作系统开发、部署、运维全流程，让操作系统更智能；另一方面，系统已支持 aarch64、x86_64、loongarch64 等主流通用计算架构，展现了其强大的兼容性与灵活性，同时支持 NVIDIA 等主流 AI 处理器，为智能时代的蓬勃发展注入了强劲动力。

5.5.1 OS for AI

- 兼容 NVIDIA 等主流算力平台的软件栈，为用户提供高效的开发运行环境。全面支持各种 AI 平台，实现 AI 软件栈全栈兼容：

  - 支持 CUDA、oneAPI 等 AI 平台框架；

■ 支持 PyTorch、TensorFlow 等训练框架，支持 Numpy、XGBoost、libxsmm 等基础算法库，确保 AI 应用在麒麟系统上高效开发与运行；

■ 支持 vllm、llamacpp、transformers、国产 chitu、dynamo 等模型推理应用，支持 llamafactory、unsloth 等模型微调应用，全方面使能大模型应用开发；

■ 支持 deepseek 开源周特性本地部署，包括高性能分布式存储文件系统 3fs、smallpond 套件、开源计算优化库 FlashMLA、DeepGEMM、EPLB、DualPipe；

■ 支持 deepseek 开源周特性容器化部署，提供基于本次发布麒麟系统根容器镜像构建的容器镜像，包括高性能分布式存储文件系统 3fs 容器镜像以及 DeepSeek 开源特性增强容器镜像；

■ 支持 opencv、oneDNN、ComputeLibrary 等计算机视觉库，支持 dlib、octave、libsvm 等 AI 数学库，构建完整的 AI 开发者生态。

● 提供基于本次发布麒麟系统根容器镜像构建的 CUDA、PyTorch、TensorFlow、vllm、chitu、llamacpp、llamafactory、unsloth、dynamo 等容器镜像，通过容器镜像天然的封装形式，提供开箱即用的使用体验。

注意：以上容器镜像不属于本产品发布组件，不提供商业技术支持

注意：容器镜像集成的 CUDA、Pytorch、Tensorflow、vllm、chitu、llamacpp、llamafactory、unsloth、dynamo、3FS 等组件及其相关依赖，来自于对应官方发布组件，与 OS 集成提供的软件包版本存在差异。

5.5.2 AI for OS

● 支持 AI 应用工具 kyCopilot，通过调用大模型及使用 RAG 技术，实现了自然语言问答与辅助编程功能，支持麒麟知识问答功能及 deepseek-r1-7B 模型调用。显著提升用户在麒麟操作系统上的工作效率，并大幅降低使用难度。

● 支持 extuner 轻量级场景调优工具，其专为麒麟操作系统设计，具备系统数据采集、系统指标分析、脱敏调优、智能调优等多种功能。支持智能调优，通过 AI 迭代运算得出最佳配置参数组合，提升客户场景应用性能，其优势在于推理时间、推理轮次可配置，用户可在短时间内得到调优指导。

● 支持 A-Tune 操作系统性能调优引擎，该工具基于人工智能技术，能够使操作系统理解业务需求，简化操作系统的调优工作，并提高应用程序的性能。

5.6 安全

Kysec 2.0 从安全框架上进行优化，扩展 LSM 形成 KSAF 以支持更多的安全接口，并允许其他模块在核外共同使用。在身份认证方面进行增强，除了口令之外，提供基于证书的 UKEY 本地和远程双因子登录认证，提高系统边界安全。完善全栈国密，strongswan、gnutls、crypto-policies、openssl 等增加国密支持，并在工具中增加基于国密算法的使用。

5.6.1 KSAF 可编程访问控制框架

KSAF 可编程访问控制框架实现了分层解耦的内核安全访问控制架构，支持定制灵活的管控策略定义，实现对应用程序和资源访问权限管控。优化 V10 版本安全功能不足问题，扩展应用场景，提升整体易用性、稳定性、可维护性等。

KSAF 可编程访问控制框架包括 ksaf-main-module、ksaf-label-manager、libksaf-policy-sync、ksaf-policy-interpreter、ksaf-dynamic-uid、ksaf-default-policy、ksaf-init、ksaf-audit-daemon、ksaf-devctl，均为麒麟自研组件。ksaf-main-module 为 KSAF 框架主驱动模块；ksaf-label-manager 负责 KSAF 框架的标记管理；libksaf-policy-sync、ksaf-policy-interpreter、ksaf-dynamic-uid 负责 KSAF 框架的策略同步；ksaf-default-policy 负责默认策略；ksaf-init 负责安全模块初始化；ksaf-audit-daemon 负责 KSAF 框架的审计；ksaf-devctl 负责提供设备管控及时生效服务，以及相关库获取设备权限。

● ksaf-main-module：基于内核安全模块堆栈化能力，实现 Kysec 2.0 中执行控制、文件保护、进程防杀、联网管控、模块防卸载、设备管控等功能需要底层基本驱动能力。

● ksaf-label-manager：KSAF 安全框架二层标记管理模块，包括标记管理服务、标记管理运维工具、标记管理接口库。主要提供标记初始化，身份管理、动态数据标记设置等功能。

● libksaf-policy-sync：KSAF 安全框架二层策略同步模块，提供策略编译和策略同

步内核的功能。

- ksaf-policy-interpreter：KSAF 安全框架二层策略解析模块，提供安全策略文件词法分析和语法分析功能。

- ksaf-dynamic-uid：KSAF 安全框架二层用户标记动态维护模块，当用户标记变化时自动进行策略更新。

- ksaf-default-policy：KSAF 安全框架二层默认策略模块，提供默认策略维护、安全框架自保护功能。

- ksaf-init：KSAF 安全框架二层开机安全初始化模块，提供系统开机过程的安全状态、标记、策略的同步功能。

- ksaf-audit-daemon：KSAF 安全框架二层核外审计服务。

- ksaf-devctl：KSAF 安全框架二层设备管控核外服务模块，提供设备管控及时生效服务，以及相关库去获取设备权限。

5.6.2 kysec2-exectl-module：执行控制内核模块

KSAF 安全框架三层执行控制内核模块，定义执行控制功能。提供上层执行控制策略使用的策略函数，包括执行控制权限检查、脚本检查、设置执行控制标记、判断多命名空间进程等。

5.6.3 kysec2-exectl-utils：执行控制核外模块

KSAF 安全框架三次执行控制核外模块，包括白名单初始化服务、执行控制标记设置相关库、白名单管理相关库以及命令行程序。主要提供标记初始化、标记设置、白名单初始化、白名单管理等功能。

5.6.4 kysec2-devctl-module：设备管控内核模块

KSAF 安全框架三层设备管控内核模块，支持细粒度设备管控，包括通过设备 id 管控、网卡名称管控功能。

5.6.5 kysec2-scene：策略统计管理服务模块

策略管理模块，该包提供了应用防护、执行控制、用户隐私数据保护、设备管控、联网管控、文件保护、内核模块防卸载、进程黑名单、静态度量、三员、文件保护箱等功能的默认策略和策略管理接口。

5.6.6 kysec2-kbox：文件保护箱内核模块

基于 KSAF 框架实现内核层文件保护箱机制，根据 ksaf 策略来对文件保护箱目录及文件进行隐藏保护，同时采用 ecryptfs 对文件保护箱目录进行加密保护。

5.6.7 kysec2-rbac-utils：管理员分权模块

KSAF 安全框架三层管理员分权模块，对系统管理命令进行划分和身份标记，分别标记系统管理员、安全管理员、审计管理员能执行，提供用户命令及接口添加、删除、查询三权命令，及三权状态设置。

5.6.8 kylin-mfa：多因子认证管理

kylin-mfa 是多因子认证管理包。用户通过 UKUI/TTY 登录系统时，先输入密码，再输入 UKEY 设备的 PIN 码 或者 输入 OTP 动态口令，认证通过则允许进入系统会话。主要包含以下功能增强：

- 新增 UKEY 本地和远程双因子用户登录认证管理。
- 新增 OTP 本地和远程双因子用户登录认证管理
- 开启/关闭多因子认证，并为用户绑定指定的 UKEY 设备或者 OTP 动态口令。

5.6.9 nettle：加密库

nettle 支持多种流行的密码学哈希函数，如 MD5、SHA - 1、SHA - 224、SHA - 256、SHA - 384 和 SHA - 512 等。主要包含以下功能增强：

- 支持国密算法 SM2、SM4。

5.6.10 gnutls： SSL/TLS 协议库

gnutls 是一个实现了 TLS（Transport Layer Security）和 SSL（Secure Sockets Layer）

协议的库。它支持多种加密算法，包括对称加密算法（如 AES - Advanced Encryption Standard）和非对称加密算法（如 RSA - Rivest - Shamir - Adleman）。主要包含以下功能增强：

- 增加 certool 工具国密算法的支持、协议层 TLS1.3 协议国密支持和通信国密支持。
- 补充缺失函数接口，提供跨版本 API/ABI 兼容能力。

5.6.11 strongswan: IPsec VPN 库

Strongswan 是一个开源的 IPsec（Internet Protocol Security）实现软件包。Strongswan 实现了 IPsec 协议的核心功能，包括封装安全载荷（ESP - Encapsulating Security Payload）和认证头（AH - Authentication Header）。主要包含以下功能增强：

- 支持国密算法，SM2、SM3、SM4、 SIGN_SM2_WITH_SM3、hmac_sm3 以及 sm2 的认证、SM2 密钥交换。
- 支持国密算法测试。

5.6.12 libtpms：TPM 模拟库

Libtpms 是一个用于软件模拟 TPM 的库。在没有物理 TPM 设备的情况下，它可以在系统中模拟 TPM 的功能。主要包含以下功能增强：

- 合入 vTPM 支持国密算法 SM3。

5.6.13 swtpm：TPM 模拟工具

Swtpm 是一个软件，用于模拟 TPM 的功能，它可以模拟硬件 TPM 的行为。在开发、测试以及研究 TPM 相关应用场景时，如果没有实际的 TPM 硬件设备，swtpm 能够很好地填补这一空缺。主要包含以下功能增强：

- 合入支持国密算法 SM3。

5.6.14 crypto-policies：加密策略管理工具

Crypto-policies 通过定义和实施加密策略来管理系统的加密功能。这些策略可以包括禁用弱加密算法、指定加密算法的优先级等：

- 新增支持国密算法 SM3。

5.6.15 gvfs：WINCE 设备管控

GNOME 桌面环境的核心组件之一，作为一个用户空间的虚拟文件系统框架，它通过虚拟化技术统一了本地与远程文件的访问接口，极大提升了文件操作的灵活性与效率：

- 支持管控 WINCE 设备的挂载、读写。

5.6.16 cups：打印机管控

专为 Unix 和类 Unix 操作系统设计的打印组件，旨在提供统一、标准化的打印接口，支持多种打印协议和驱动程序。

- 支持管控打印机。

5.6.17 sane-backends：扫描仪管控

为各种扫描仪硬件提供统一的编程接口，负责与实际的扫描仪设备进行通信，实现扫描功能的底层支持。

- 支持管控扫描仪。

5.6.18 selinux-policy：selinux 默认策略

SElinux 的核心策略包，提供了操作系统 selinux 安全策略的定义和规则。

- 可信启动支持三权 se 策略。
- 新增 kguard 入侵检测 se 策略。

5.6.19 libselinux/libsemanage：安全用户标记

SELinux 系统中的一个核心的 C 语言库，用于管理和操作 SELinux 策略模块。

- 新增支持 secadm 和 auditadm 安全用户标记。

5.6.20 kmod：ko 模块加载管控

Linux 系统中用于内核模块管理的基础软件包和工具集合。

- 去除对 ko.xz 的上层检测逻辑。

5.6.21 pam/shadow/passwd：密码及登录

1. PAM（Pluggable Authentication Modules）

PAM 是系统的模块化认证框架，提供灵活的身份验证机制，主要功能包括：多因素认证：支持密码、数字证书（如 SM2 国密算法）、生物识别（指纹/人脸）等组合认证。

- 密码复杂度控制：通过 pam_pwquality.so 模块强制密码策略，如最小长度（默认 12 位）、需包含大小写字母/数字/特殊字符等。

- 登录失败处理：限制连续失败次数（如 5 次锁定账户），并记录审计日志至/var/log/secure。

- 安全增强：集成国密算法支持，并默认禁用弱加密协议（如 DES)。

- UID 唯一性检查: 用户登录时 UID 唯一性检查。

2. shadow

Shadow 工具集负责用户密码的安全存储与管理，核心特性如下：

- 影子密码机制：加密后的密码哈希存储在/etc/shadow（仅 root 可读），避免/etc/passwd 泄露风险。

- 密码策略强制：通过/etc/login.defs 定义密码有效期（如 PASS_MAX_DAYS 90）、过期警告天数（PASS_WARN_AGE 7）等。

- UID 唯一性检查：在 useradd/usermod 时验证 UID 全局唯一，冲突时返回错误。

- 命令支持：useradd/usermod/userdel/chage。

3. passwd

Passwd 是用户密码修改的核心工具，主要功能包括：

- PAM 集成：调用 pam_cracklib.so 检查密码复杂度，拒绝简单密码。

- 密码历史记录：通过/etc/security/opasswd 防止重复使用近期密码。

- 权限控制：普通用户仅能修改自身密码，root 可重置任意账户。

- 国密算法支持：可选 SM3 哈希加密，替代默认的 SHA-512。

5.6.22 libchkuid：用户唯一性检查库

- Libchkuid 是专注于 UID 唯一性检查的接口库，主要目标是为了在系统上实现用户 UID 唯一性保护功能，即一个 UID 在操作系统的整个用户管理生命周期过程中只能被一个用户使用，这就意味着即使一个用户被删除后，分配给此用户的 UID 也不能再次分配给其他用户使用，这样设计的目的是为了有效避免此用户的遗留文件被非法访问，确保用户数据隔离和安全。

5.6.23 kysec-utils/libsecurity1/kysec-common/kysec-daemon/kysec-sync-daemon/security-switch：安全增强子模块 1.0

Kysec 1.0 上层接口组件包，提供执行控制、网络保护、文件保护等 sdk 接口。

- 新增 Kysec 组件，适配 ksaf 框架。

5.6.24 audit-status-libs：审计接口库

audit-status-libs 是一个用于管理系统审计状态的动态库。

- 系统审计状态管理动态库提供审计状态查询、审计状态设置接口。

5.6.25 sm-enhancement：安全套件授权管理工具

安全套件授权管理工具和 SDK，提供了安全套件使用的功能接口以及授权验证机制。通过授权后的程序可以调用安全套件接口，以配置设备管控、文件保护、进程保护、内核模块防卸载、壁纸管控、软件包防卸载等功能的策略。

5.6.26 kylin-log-viewer：日志查看器

日志查看器是一款系统日志集中展示工具，提供日志解析和分类显示功能。主要包含以下功能增强：

- 适配 ukui 框架。
- 适配 Kysec 2.0 日志详情。
- 优化麒麟安全日志显示级别。

- 优化数据刷新时数据加载弹窗自动退出。

5.6.27 box-utils/box-manager：文件保护箱

文件保护箱是基于内核级数据隔离机制的保护工具，提供用户间数据隔离和加密保护功能，支持国密算法，实现一箱一密、一文一密的细粒度控制，保障用户数据安全。主要包含以下功能增强：

- 更新 ksaf 策略，提供更严格的安全限制。
- 优化部分 UI 界面问题。

5.6.28 ksc-defender：安全中心

安全中心是一款构建安全防护并行的图形化管理工具，集安全加固、账户保护、可信度量、安全工具等功能于一体，全面保障系统运行环境的安全。主要包含以下功能增强：

- 更新安全加固界面。
- 更新账户保护功能。
- 新增可信度量功能。
- 新增安全工具功能，包含应用程序执行控制、文件防篡改、内核模块防卸载、进程防杀死、应用联网控制等。

5.6.29 security-reinforce：安全加固

安全加固提供安全服务、内核参数、安全网络、系统命令、系统审计、系统设置、潜在危险、文件权限、风险账户、磁盘检查、密码强度、账户锁定、系统安全、系统维护、资源分配等多维度的扫描与一键加固，及时发现并处理系统安全隐患。主要包含以下功能增强：

- 修复禁用 ctrl+alt+del 组合键失败。
- 修复用户登录 ftp 后访问目录权限正确 加固还原后源文件备注的信息被删除。
- 修复设置 SSH 安全协议还原后将注释项也删除了。

- 修复限制仅允许系统管理员进入维护模式，实际加固失败。
- 修复禁止 root 登录 VSFTP，扫描不成功。
- 修复密码策略里回文检查参数错误。
- 修复未安装 quota 和 libcgroup，未扫出检查系统资源使用控制待加固项。
- 修复禁用不必要别名需要执行 newaliase。
- 更新基线描述。
- V11 2503 适配空闲时间锁屏加固项。
- 使用权限调整，仅 root 用户有安全加固的使用权限。

5.6.30 usbguard：设备管控交互式工具

USBGuard 是一个用于 USB 设备访问控制的工具。它允许管理员对 USB 设备的访问进行授权管理。主要包含以下功能增强：

- 修复全部设备管控策略查询-授权提示转储、设备授权取消授权大概率转储问题。
- 修复 usbguard 服务无法正常启动问题。
- 去除 usbguard-selinux 包，策略已在 selinux-policy 统一管理。
- 修复关闭设备管控需要插拔生效。
- 修复导入错误格式策略提示核心已转储。
- 修复设备管控事件通知无状态变更弹窗。
- 修复放行部分 usb 接口提示核心已转储。
- 默认放行人机交互设备及 USB Hub 设备。

5.6.31 usbguard-notifier：设备管控交互式工具

Usbguard 设备管控分包，提供设备插入/退出时显示弹窗。主要包含以下功能增强：

- 修复设备管控事件通知无状态变更弹窗。

- 修复 usb 设备管控事件通知图标未显示，提示不友好。

5.6.32 pesign/nss：文件签名工具

Pesign 是一个用于文件签名的工具。它能够对各种类型的文件进行签名操作，确保文件的完整性和来源可靠性。nss 是一个提供网络安全服务的库，其中包含了丰富的密码学功能。主要包含以下功能增强：

- 修复同名证书导入后不可使用的修复补丁。

5.6.33 libkydima：动态度量管理工具

libkydima 是自研的动态度量管理工具，包含度量策略查询与配置命令工具，用于用户查询或配置动态度量状态及策略；开机策略初始化服务，用于在开机时根据用户配置开启动态度量功能并同步下发固化策略到组件中。

5.6.34 lkrg-kyextend：动态度量内核模块

lkrg-kyextend 是动态度量内核模块，提供进程、内核、系统调用表等度量机制。主要包含以下特性：

- 进程度量任务线程，用于度量及管控进程代码段及只读数据段，实现进程篡改的告警或事后终止已损坏进程。

- 内核及内核模块度量任务线程用户度量内核关键资源及内核模块只读数据段代码段，提供内核太关键资源篡改告警能力。

- pcr 扩展组件，用户处理度量日志 pcr 扩展提供可信报告基本能力。

5.6.35 rootca-gov-cn：国家电子根证书管理工具

rootca-gov-cn 是自研的国家电子根证书管理工具，增加对二级证书的管理。主要包含以下功能增强：

- 修复 crash 问题和堆积 CI。

- 解决普通用户权限提示不友好问题。

- 解决 删除 GDCA 目录，重新导入证书后，普通用户查询证书列表失败问题。

5.6.36 kytrust-bima：可信启动管理工具

kytrust-bima 是可信启动管理工具，提供功能开关、基准值初始化、查询度量报告。

5.6.37 libkytrusted-security：可信启动统一接口层

libkytrusted-security 是可信启动统一接口层，提供对 TPM/TCM/KYEE 等不同设备的访问接口，以及状态修改、基准值生成等功能实现。

5.7 UKUI 4

UKUI 是由麒麟团队开发的基于 Linux 发行版的轻量级桌面环境，从用户使用角度出发，增加了全屏开始菜单、个性化任务栏，夜间模式等功能，最大程度地满足了不同用户对易用性、个性化的需求。同时对部分图形软件工具进行了全新的设计及功能优化，除满足用户的实际办公需求外，在易用性等方面也进行了升级。UKUI 将视觉和交互舒适自然的结合在一起，在主流硬件平台上拥有更美观的 UI 界面、更友好的一致性交互体验。目前 UKUI 已经更新到版本 4。

- 重新设计的系统登录和锁屏，提供更为清晰的用户登录入口。
- 全新设计的文件管理器，从底层开始进行了彻底的重构，着重增加了稳定性。支持图标视图和列表视图，满足用户对文件管理的需求。
- 全新升级的开始菜单，不仅可以查看并管理系统中已安装的应用，在菜单中使用分类导航或搜索功能可以快速定位应用程序，还提供了全屏模式。两种模式均支持搜索应用、设置快捷方式等操作，并支持快速打开文件管理器，设置和进入关机界面等功能。
- 多任务视图可以自由划分创建工作区，为每项工作建立独立空间。显示任务视图时，可将任务窗口拖拽到其它工作区。

5.8 网络

5.8.1 iptables：用户态防火墙管理

Iptables 是 Linux 系统中常用的防火墙工具，用于配置和管理内核的网络包过滤

规则。它基于 Netfilter 框架，支持对进出主机的网络流量进行匹配、过滤、转发、NAT 等操作。iptables 按照表（filter、nat、mangle 等）和链（INPUT、OUTPUT、FORWARD 等）结构组织规则，广泛应用于网络安全控制、端口转发、防火墙策略配置等场景。新版支持与 nftables 协同工作。

- 支持 xlat 表扩展。
- nftables 后端兼容性增强。
- 优化了规则遍历和输出生成的逻辑。
- 新增 --enable-profiling 配置选项，便于使用 gcov/gprof 进行代码性能分析。
- SCTP 扩展支持更多 chunk 类型。
- 在 ebtables-nft 中支持 -p Length，适用于 802.3 扩展。

5.8.2 firewalld：动态防火墙管理服务

Firewalld 是 Linux 系统中的动态防火墙管理工具，基于 zones 和 services 概念，支持即时添加、修改和删除规则，无需重启服务。它通过封装 iptables 或 nftables，简化了复杂的防火墙配置，支持 IPv4/IPv6、接口绑定、端口转发、富规则等功能，适合灵活防护需求。

- 支持 nftables 后端（默认后端变更），替代传统 iptables 的新内核防火墙框架。
- 支持富规则 (Rich Rules) ，增加了对更多匹配条件的支持。
- 动态规则更新更加稳定，减少了规则重载时的中断。
- 支持 ICMP 阻塞和过滤功能，增强了对 ICMP 类型和代码的阻塞控制能力。

5.8.3 networkManager：网络管理工具

NetworkManager 是一个为系统自动连接到网络提供检测和配置功能的软件。

- 支持 mptcp 协议。
- 支持 ovs 配置选项。

5.8.4 mptcpd：用户态守护程序

Mptcpd 服务是 mptcp 协议的用户态守护进程，负责 mptcp 协议的功能配置、链接管理和状态监控等。mptcpd 软件包支持如下功能：

- 提供路径管理策略配置功能，将用户自定义管理策略下发给内核。
- 监控本地可用的网络接口和地址变化。
- 启动、关闭和管理子流。

5.8.5 dhcp：动态主机配置协议

DHCP 是一种用于 IP 网络的地址管理协议，通过该协议，DHCP 服务器动态地向网络上的每个设备分配 IP 地址和其他网络配置参数，以便这些设备能够与其他 IP 网络进行通信。

- 提供了创建连接和等待操作完成的定时功能。
- BIND 库更新到 9.11.36 版本。
- 支持 RFC 8925 中指定的 v6-only-preferred 选项。

5.8.6 bind：DNS 协议的实现工具

BIND（Berkeley Internet Name Domain）是 DNS（域名系统）协议的一种实现。BIND 包括一个 DNS 服务器（名为 named），它将主机名解析为 IP 地址；一个解析器库（应用程序与 DNS 交互时使用的例程）；以及用于验证 DNS 服务是否正常运行的工具。

- lnslookup 默认查找 AAAA 和 A 记录。
- 通过为基于流的传输分配适当大小的发送缓冲区来减少内存消耗。

5.8.7 iperf3：网络性能测试工具

Iperf3 是一款用于测量服务器网络最大带宽的工具。它允许用户指定协议、缓冲区和时间等参数，以便进行精确的网络性能测试。

- iperf3 支持 mptcp 协议。

- 支持 RFC 5865，对 QoS（服务质量）进行更好的兼容。
- 在构建时优先选择 OpenSSL3 安全协议。

5.8.8 gazelle：高性能用户态网络协议栈

Gazelle 是一款高性能用户态协议栈，专注于加速数据库网络性能。它基于 DPDK 实现用户态直接读写网卡报文，利用共享大页内存和轻量级 LwIP 协议栈，显著提升应用的网络 I/O 吞吐能力。Gazelle 支持报文零拷贝、无锁设计、灵活的扩展能力和自适应调度，同时兼容 POSIX 接口，实现零修改，适用于各种应用场景。银河麒麟高级服务器操作系统 V11 2503 gazelle 支持 1.0.2，兼容适配 lwip 2.2.0 和 dpdk 23.11 版本，主要特性如下：

- gazelle 吸取 lwip 和 dpdk 高版本特性，兼顾高性能与通用性。这里需要注意的是 lwip 仅配合 gazelle 使用，并非单独作为库而运行。
- 兼容 lwip 新版本对 IGMPv3/MLDv2 路由组播协议支持，丰富用户态网络高性能协议库。
- 支持 select 的阻塞式场景，扩充 posix api 兼容功能，丰富网络场景支撑能力。
- 支持命令行工具对流量状态信息的查询，简化旁路网络的运维管理。
- 支持 gazelle 启动多个进程，监听不同的端口在不同的队列上，实现业务多扩展性，丰富网络场景。

5.8.9 dpdk：高性能网络数据面开发套件

DPDK 全称 Date Plane Development Kit，是专注于数据面软件开发的套件。它提供了一个强大的框架，可提高各种 CPU 架构的数据包处理速度，是快速开发高速数据包网络应用的关键。

- DPDK 版本升级到 23.11，对 i40e、iavf、cpfl 等驱动进行功能支持项升级，并新增对用于 AMD EPYC 处理器的 amd-pastate 驱动的支持，实现用户态驱动能力延展，丰富用户态驱动生态库。
- 扩展 ADM 处理器电源函数的支持，新增 MONITORX/MWAITX 指令，实现对 AMD 处理器的功耗优化。

● 新增数据包类型流匹配功能。添加了 RTE_FLOW_ITEM_TYPE_PTYPE 以允许匹配 L2/L3/L4 和 mbuf 数据包类型中定义的隧道信息。提升网卡与多核处理器、多任务系统配合能力，提升 IO 处理效率。

● 新增 rx 缓冲区最大值设置，减少对内存池空间的浪费，提升程序运行性能。

5.8.10 openvswitch：虚拟交换机

Open vSwitch（OVS）是一款生产级的多层虚拟交换机，基于开源的 Apache 2.0 许可证发布。它旨在通过可编程扩展实现大规模网络自动化，同时仍支持标准的管理接口和协议（如 NetFlow、sFlow、IPFIX、RSPAN、CLI、LACP、802.1ag 等）。此外，它的设计支持跨多台物理服务器的分布式部署。

openvswitch 版本升级到 3.2，主要提升了性能、监控能力和协议支持，包括无锁 Meter 优化、DPDK 硬件加速（支持超过 34Gbps 的 QoS/限速）、PMD 线程睡眠调优，以及 IPFIX 可配置监控和 Linux 6.2+内核级 upcall 统计。新增了对 SRv6 隧道和 SCTP 连接跟踪的支持，并优化了路由（智能源地址选择）和连接跟踪管理（可调 CT 垃圾回收）。此外，移除了对 Python 3.6 以下版本的支持，并改进了 OVSDB 集群的 schema 转换性能。

5.8.11 sysmonitor 系统监控工具

sysmonitor 是一款系统监控软件，负责监控操作系统运行过程中的异常，将监控到的异常记录到系统日志，方便使用者定位系统异常问题。sysmonitor 可以监视系统资源的使用情况，如 CPU、内存、磁盘等；监控网卡状态，系统运行过程中可能出现人为原因或异常而导致网卡状态或 IP 发生改变，对网卡状态和 IP 变化进行监控；定期监控系统中关键进程，当系统内关键进程异常退出时，自动尝试恢复关键进程；监控 ext3/ext4 文件系统是否有错误码；监控文件增删等。通过实时监控、异常记录、服务化部署等功能，sysmonitor 极大程度上节约了运维成本，提升了对服务器操作系统的运维能力。

5.8.12 oeAware 动态调优框架

oeAware 是实现低负载采集感知调优的框架，将调优拆分为采集、感知和调优三层，每层通过订阅方式关联，各层采用插件式开发。oeAware 以插件的形式管理采集、

感知和调优功能，可以动态开关插件，从而可以根据不同业务场景制定针对性的调优策略。具备低负载采集和动态调优特性。

5.9 存储

5.9.1 xfsprogs：XFS 文件系统管理工具集合

xfsprogs 是一组用于管理 XFS 文件系统的实用工具，提供了从文件系统创建到维护的全方位支持。这些工具包括，文件系统格式化，挂载，检查，修复，诊断，以及其他用于管理 XFS 文件系统的实用工具。

- 支持 xfs_db 从外部设备读取数据，是转储元数据到外部设备的基础。
- 支持 liburcu，优化锁设计，提升原子变量访问性能。
- 支持 xfs_repair 第 6 阶段并行化处理，提升修复性能，缩短文件系统损坏修复时间。
- 支持 rmap，跟踪数据块使用情况，确保数据的完整性和一致性。
- 支持 Large extent counts 特性，使用 48 位表示文件的 extent 个数，对大文件的操作支持更完善。
- 支持日志打印 ATTRI 和 ATTRD，使得日志信息更清晰。
- 支持 inobtcount，减少大型 XFS 文件系统挂载时间。
- 支持 bigtime，能够支持更长的时间范围。

5.9.2 bcachefs-tools：bcachefs 文件系统管理工具集合

Bcachefs-tools 是一组用于 bcachefs 文件系统的管理工具集合。bcachefs 是一种高性能、可扩展的文件系统。bcachefs-tools 提供了全面的管理和维护 bcachefs 文件系统的功能。

- 新增 bcachefs-tools 工具。
- 支持 COW 技术，提高写入操作效率，有助于避免数据损坏和一致性问题。
- 支持多设备管理，能够管理多个物理设备，并支持动态添加和移除设备，提供

了数据冗余、性能提升。

● 支持快照，能够创建文件系统状态的快照，并支持快速回滚到先前的文件系统状态。

● 支持数据压缩，提高存储空间的使用率。

● 支持数据加密，保护存储在文件系统中的数据安全性。

● 支持在线修复，文件系统能够在运行时进行在线修复，处理文件系统中的一致性问题而无需停机或重启。

● 支持动态空间分配，bcachefs 能够动态管理存储空间的分配和释放，以适应不断变化的存储需求。

● 支持多版本文件系统，允许用户在文件修改后仍能够访问先前版本的文件数据。

● 支持指定单个设备挂载 bcachefs 文件系统，不再产生告警信息，提高产品易用性和实用性。

5.9.3 spdk：存储性能开发工具包

SPDK (Storage Performance Development Kit)提供了一组工具和库，用于编写高性能、可扩展的用户模式存储应用程序。它通过将所有必要的驱动程序移到用户空间并以轮询模式运行而不是依赖中断来实现高性能，这避免了内核上下文切换并消除了中断处理开销。

支持 NVMe over vfio-user，允许 SPDK 将完全模拟的 NVMe 设备呈现到虚拟机中，虚拟机可以利用其现有的 NVMe 驱动程序与设备进行通信，并且数据可以使用共享内存高效地传输到 SPDK 或从 SPDK 传输。

● 增加对 BPF 跟踪的支持，与原有的跟踪库 libtrace 相比，功能更加强大，可以动态链接，而无需在代码中定义探测器。

● 在 NVMe-of TCP Target 中增加对零拷贝操作的支持。

● 增加了支持 DAOS 的新 bdev 模块，在 DAOS DFS 之上创建 SPDK 块设备，使用每个设备通道的独立池和容器连接，提高了 IO 吞吐量。

- 新增 ublk 库，可以使用 V11 2503 6.6 内核中添加的 Linux ublk 框架将 SPDK 块设备公开为 Linux 内核块设备。基于 io_uring 和 blk-mq 来帮助提高性能和扩展性。

- 增加了 nvmf 传输从 iobuf 池中申请缓冲区的功能。nvmf 库与 bdev 层共享相同的内存池，减少了总体内存使用量。

- 增加了 JSON-RPC 2.0 客户端，以简化与 SPDK 的通信。

- RAID bdev 模块支持 RAID1 和 RAID5F 级别的重建。

- 增加 ctrlr_lock 锁避免启动 CUSE 时发生 core dump 问题。

5.9.4 glusterfs：glusterfs 文件系统

GlusterFS 是一个具有高可扩展性的开源分布式文件系统，能够将多个服务器上的存储资源整合为一个统一的全局命名空间，供客户端透明访问。它基于用户态的模块化架构，不依赖集中式元数据服务器，从而简化了部署和运维。GlusterFS 支持副本、仲裁等多种数据冗余与容错机制，具备良好的高可用性和可靠性。

- 支持随机选择 brick 的端口：优化卷启动流程，显著缩短系统启动时间。

- 自愈性能提升：通过增大每个自愈窗口的数据传输量，提升并发修复能力，加快数据自愈速度，尤其适用于大规模数据或高负载环境。

- 集成 io_uring 支持：利用 Linux 新一代异步 I/O 接口，显著提升 I/O 操作的性能，特别是在高并发场景下效果显著。

- 支持最多 5000 个卷并发运行：满足超大规模集群对多租户或多任务的存储需求。

- 新增日志轮换机制：支持用户自定义快照日志的轮换策略，提升日志管理灵活性。

- Hin-Arbiter 集成进 GD1 卷类型：增强集群在脑裂场景下的数据一致性，减少资源消耗，提升系统整体稳定性。

- 支持 ZFS 快照的原生集成：提升快照性能、保证数据备份的一致性。

- 基于命名空间的配额管理：允许针对不同命名空间设置独立的存储配额，实现

更灵活、精细的存储资源控制。

5.9.5 etmem：内存分级扩展组件

Etmem 内存垂直扩展技术，通过 DRAM+内存压缩/高性能存储新介质形成多级内存存储，对内存数据进行分级。在使用时运行用户态的 etmemd 进程，对业务进程的内存数据进行扫描获取内存页面的访问情况，并通过淘汰算法对内存页面的冷热进行分级，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，从而实现内存成本下降。

- 支持 clang 编译，极大加快了程序编译速度。
- 增加 debug 调试功能。

5.9.6 mdadm: Linux 软 RAID 管理工具

Mdadm 是一个管理 RAID 阵列的命令工具，提供了创建、管理、监控 RAID 阵列的功能。

- 修复"mdadm --incremental"命令潜在的空指针问题。
- 修复"mdadm -f"命令主动拔盘造成的 RAID 0 不可用问题。
- 修复 RAID 1 增加新磁盘可能失败的问题。
- 修复无软 RAID 设备时 mdmonitor 服务自启动问题。

5.9.7 lvm2：逻辑卷管理器

LVM2 (Logical Volume Manager Version2)是从物理设备创建虚拟块设备的工具。一个卷组(VG)是一个或多个物理设备的集合，每个物理设备称为 PV。逻辑卷 LV 是系统或应用程序可以使用的虚拟块设备。LV 中的每个数据块存储在一个或多个 LV 上，根据 DM 在内核中实现的算法，在 VG 中创建 PV。

- 增强 raid 功能的完整性，增强 lvdisplay 显示 raid 可用，以及允许在 raid+LV 上写 cache。
- 支持使用 BLKZEROOUT 清理设备，支持擦除 LV 时的中断，支持中断 bcache 等待，支持调整缓存卷的大小等特性。

- 增加对 writecache metadata_only 和 pause_writeback 设置的支持。

- 增加 vdoimport 工具，支持 VDO 卷的转换，增加对 VDO 异步不安全写策略的支持，以及在线重命名 VDO 池。

- 增加 fsadm 的错误处理，并处理正确的 fsck 结果，以及修复 fsadm 中未绑定变量使用的问题，使用 getsize64 支持 fsadm 处理 blockdev。

- 提升 lvremove 和 vgremove 命令的性能。

- 修复擦除转换 LV 的问题，修复扫描时内存泄漏的问题，修复 bcache 等待 IO 完成故障磁盘的问题，修复使用历史 LV 处理选择时的段错误问题。

5.9.8 multipath-tools :多路径管理工具

Multipath-tools 软件包提供 multipath 工具和 multipathd 守护进程，用于管理 dm-multipath 设备。multipath 可以检测和设置多路径映射。multipathd 会自动设置多路径映射，监控路径设备的故障、移除或添加，并对多路径映射进行必要的更改，以确保映射设备的持续可用性。

- 对 Linux TCM (LIO)目标使用 directio 路径检查器。

- 硬件表更新： PowerMax NVMe、Alletra 5000、FAS/AFF 和 E/EF。

- 对 NVMe/TCP 路径强制设置 queue_mode bio。

- 由于许可证冲突，multipathd 不再使用 libreadline，因为 readline 已将许可证改为 GPL 3.0，这与 multipath-tools 代码库中部分代码的 GPL-2.0 唯一许可证不兼容。因此，multipathd 中的命令行编辑功能默认是禁用的。在编译过程中，可以通过设置 READLINE=libedit 来使用 libedit 代替 libreadline。也可以设置 READLINE=libreadline。只有不包含 GPL-2.0 代码的新辅助程序 multipathc 与 libreadline 或 libedit 链接。multipathd -k 现在会执行 multipathc。

- 作为分离许可冲突代码工作的一部分，multipath 已被拆分为 libmultipath 和 libmpathutil。后者可以与 GPL-3.0 代码连接，而不会产生许可冲突。

- 优化 multipath -u 和 multipath -U 的启动速度。

- 在有大量别名条目的系统中加快查找别名的速度。

- 对于 Clariion/Unity 存储阵列，使用 emc_clariion 检查器。
- 现在可以在 multipath.conf 的 overrides → protocol 部分按协议设置 dev_loss_tmo、eh_deadline 和 fast_io_fail_tmo 属性。
- config_dir 和 multipath_dir 运行时选项自 0.8.8 起已被标记为弃用，现分别由编译时选项 configdir= 和 plugindir= 取代。
- 不再支持 getuid_callout。
- 重新编写了 uevent 过滤和合并代码，以避免 uevent 处理过程中的人为延迟。
- 修正了 man 手册中 prio_args 和 find_multipaths 相关的描述错误。
- 新增路径 delayed 状态计数功能。

5.9.9 btrfs-progs:btrfs 文件系统管理工具

Btrfs-progs 提供用户空间实用程序来管理 btrfs 文件系统，包括修复、修改、创建等。

- libbtrfsutil 许可证改为 LGPL v2.1+。
- mkfs 新增选项 -R 用于运行时选项（例如，挂载时启用），现在支持 free-space-tree。
- mkfs 支持 zoned 模式，支持获取 zoned 设备上的元数据。
- mkfs 允许创建退化的 RAID0 和 RAID10。
- mkfs 支持 block-group-tree。
- check 新增选项 -o inode_cache 用于移除 inode 缓存中的残留。
- convert 增加--uuid 选项以复制、生成或设置给定的 uuid 值。
- qgroup 增加子命令 clear-stale，删除没有子卷的 qgroup。
- rescue 新子命令 create-control-device。
- rescue 新增子命令 clear-uuid-tree 以修复由错误 uuid 子卷键导致的挂载失败。
- subvolume delete 新增新选项 --dry-run。

- 新命令 inspect-internal map-swapfile 用于检查 swapfile 及其用于休眠的 swapfile_offset 值。
- 支持在读取 RAID5/6 时自动修复。
- 支持撤销 filesystem resize 和 device remove。
- mkfs 的 zone 重置和丢弃将在所有设备上并行完成。
- check 能够重置 dev_item::bytes_used 计数。
- subvol delete 允许通过 ID 删除子卷。
- send 支持 v2 协议。
- 在 x86_64 上以回退模式实现加速哈希算法。

5.9.10 e2fsprogs:ext2/3/4 文件系统管理工具

E2fsprogs 软件包包含许多工具，可供用户创建、检查、修改和更正 ext2/3/4 文件系统。

- 添加对 orphan_file 特性的支持，可以加快并行删除或截断大量文件的速度。
- mke2fs 现在支持扩展选项 "assume_storage_prezeroed"，该选项会使 mke2fs 跳过对日志和 inode 表的清零操作，并将 inode 表标记为已清零。
- chattr 和 lsattr 现在支持 FS_NOCOMP_FL 标志。
- 支持 stable_inodes（COMPAT_STABLE_INODES）功能：此功能支持 fscrypt siphash 算法，该算法根据 UUID 和 inode 编号计算加密的初始向量。
- 支持同时启用文件系统加密和 casefold 功能的文件系统。
- fuse2fs 程序新增了 -o norecovery 选项：该选项将抑制任何可能需要的日志重放，并以只读方式挂载文件系统。
- 支持在 chattr 和 lsattr 命令中使用 x 属性来设置/获取特定文件的 DAX 支持。
- 支持 gnu.* 扩展属性命名空间。

● 允许 tune2fs 和 e2label 使用 ioctl 来设置挂载文件系统的标签和 UUID，此方式比通过写入块设备修改超级块更可靠。

● e2fsck 现在会在加密文件与其包含目录的策略不同的情况下找到并修复文件系统损坏问题。

● e2fsprogs 程序（尤其是 fuse2fs）现在可以在不清除哈希树索引的情况下更新哈希树目录。

● mke2fs 现在设置 s_overhead_cluster 字段，以便内核在挂载时不需要计算它，这加快了挂载非常大的文件系统的速度。

● mke2fs 支持批量清零 inode 列表，优化了大容量磁盘的初始化速度。

● 引入 fast_commit（COMPAT_FAST_COMMIT）功能，为 fsync(2) 系统调用提供了更细粒度的日志记录，改善了延迟。

● 修复了在使用直接 I/O 时，如果使用了回弹缓冲区并且出现短读，可能导致互斥锁不平衡的问题。

5.9.11 open-iscsi：iSCSI 协议 initiator 工具

Open-iSCSI 是根据 RFC3720 iSCSI 协议实现的高性能 initiator 程序。它使得访问 SAN 上的存储不再只能依赖 Fibre Channel，也可以通过以太网将存储设备作为块存储访问。Open-iSCSI 使得远程存储看起来像本地磁盘，可以被操作系统直接管理。它的主要组成部分有 iscsi initiator、iscsid 守护进程和 iscsiadm 工具。

● 支持最新 iSCSI 协议规范，包括对最新 iSCSI 标准的命令集和功能的支持，确保能够与最新的存储设备和系统无缝协作，特别是在高并发和大数据量传输的场景下提高了数据传输速度。

● 增加认证和加密机制，除了基本的 CHAP 认证，还增加了对更高级别认证的支持，如双因素认证和更强的密码加密算法，提高了数据在传输过程中的机密性和完整性，防止未经授权的访问和数据泄露。

● 动态负载均衡优化，引入了更先进的动态负载均衡策略，能够根据路径的实时状态（如带宽、延迟）动态调整数据流的分配，以最大化传输性能。

● 优化故障切换，在多路径 I/O 中，当一条路径出现故障时，能够更快速地切换到备用路径，提高了存储系统在面对网络波动和设备故障时的稳定性，确保数据传输的连续性。

● 新增策略配置，增加了对多种 IO 策略的支持，如轮询、最小队列深度、最少字节数等，用户可以根据实际需求选择最适合的策略，更简单的配置和优化存储系统。提高了策略配置的灵活性，提升管理效率。

● 新增路径优先级和权重配置，允许用户为不同的路径设置优先级和权重，使得关键路径在数据传输中获得更高的优先级，以提高整体系统的性能和可靠性。

5.9.12 ceph：分布式存储

Ceph 是一个分布式存储系统，设计用于构建可扩展的存储服务，支持大规模的数据存储和处理。它提供了灵活的存储解决方案，包括对象、块和文件系统存储，能够满足各种应用场景的需求。

● 支持新的 publish/subscribe 基础架构，允许 RGW 将 events 推送至 serverless frameworks。

● 支持 pool 中的独立 image namespaces，以便进行租户隔离。

● 引入了 RocksDB Sharding，减少了磁盘空间需求。

● mClock 调度程序（Quincy 中的默认调度程序）已进行重大可用性和设计改进，以解决回填缓慢的问题。

● OSD 通过冲突请求抢占清理可减少尾部延迟。

● 新的 Web 前端(Beast)已取代 civetweb 成为默认前端，从而提高了整体性能。

● 新的 rbd perf image iotop 和 rbd perf image iostat 命令为所有 RBD 映像提供类似 iotop 和 iostat 的 IO 监视器。

● 新的 cephfs-shell 工具可用于处理无需挂载的 CephFS 文件系统。

● 新增 cephfs-top 工具用于查看 CephFS 客户端性能指标。

5.9.13 gdisk:磁盘分区工具

Gdisk（由 gdisk、sgdisk、cgdisk 组成）是一组文本模式分区工具，适用于 GPT（GUID Partition Table）分区表的管理，主要用于划分容量大于 2T 的硬盘。

- 添加了对齐分区端点的支持，此功能会影响在 gdisk 中使用 n 时的默认分区大小和 cgdisk 中的默认分区大小，并且它由 sgdisk 中新的-l 选项激活。

- 增加了对磁盘太小的检查，如果发生这种情况，程序现在就会中止。

- 支持将分区标签数据的字节编码交换到 gdisk 和 sgdisk，此功能可以纠正由 gdisk 1.0.7 或更早版本在 big-endian 计算机上创建的错误编码的分区名称。

5.9.14 nfs-utils:NFS 协议文件系统工具集合

Nfs-utils 提供了实现 Network File System（NFS，网络文件系统）协议的工具和服务。NFS 允许不同计算机之间通过网络共享文件系统，使得用户可以像访问本地文件一样访问远程文件。nfs-utils 主要包含的组件功能有：NFS 服务端和客户端工具、NFS 配置工具、rpc.statd 等守护进程、NFS 监控和日志调整等。

- 新增 libnfsidmap 和 nfs-utils-min 两个子包，libnfsidmap 提供的是 NFSV4 名称(格式为 user@domain)和用户标识(UID/GID)建立映射等功能，nfs-utils 安装依赖 libnfsidmap，nfs-utils-min 旨在提供最小化的 nfs-utils 实用功能。

- 优化 nfs-blkmap 服务启动流程，解决服务启动失败问题，提升服务的稳定性。

- 使用 gss-proxy，允许不同域之间的应用程序进行安全通信和身份验证，提高 nfs-utils 的安全性。

5.9.15 samba：SMB 协议文件共享工具

Samba 是 Linux 和 UNIX 系统上实现 SMB 协议的一个免费软件，由服务端及客户端程序构成。既可以用于 windows 与 Linux 之间的文件共享，也可以用于 Linux 与 Linux 之间的资源共享，主要由以下部分组成：smbd、nmbd、Winbind、Samba Client Tools、CTDB 等。

- 优化了源码包的生成速度，提升了编译速度，提高了效率。

- 新增 samba-client-libs 和 samba-dc-libs RPM 包，为 samba 客户端和域控制
- 提供所需的库文件和支持。
- 优化 krb5 协议的支持，提升 samba 软件的安全性。

5.10 编译工具链

5.10.1 gcc :编译器工具集合

GCC 是 GNU Compiler Collection 的简称，是几种主要编程语言的编译器的集成发行版：C、C++、Objective-C、Objective-C++、Fortran、Ada、D 和 Go，并具备跨平台性、广泛的处理器架构支持以及强大的优化功能。

- GCC 版本升级到 12.3，默认语言标准从 C14/C++14 升级到 C17/C++17 标准，支持 AVX512 FP16 等硬件架构特性。
- 支持结构体优化，指令选择优化等，充分使能 aarch64 架构的硬件特性，运行效率高，在 SPEC CPU 2017 等基准测试中性能大幅优于上游社区的 GCC 10.3 版本。
- 支持自动反馈优化特性，实现应用层 MySQL 数据库等场景性能大幅提升。
- 支持 aarch64 架构下 SVE 矢量化优化，在支持 SVE 指令的机器上启用此优化后能够提升程序运行的性能。
- 支持内存布局优化，通过重新排布结构体成员的位置，使得频繁访问的结构体成员放置于连续的内存空间上，提升 Cache 的命中率，提升程序运行的性能。
- 支持冗余成员消除优化，消除结构体中从不读取的结构体成员，同时删除冗余的写语句，缩小结构体占用内存大小，降低内存带宽压力，提升性能。
- 支持数组比较优化，实现数组元素并行比较，提高执行效率。
- 支持 aarch64 架构下指令优化，增强 ccmp 指令适用场景，简化指令流水。
- 支持自动反馈优化，使用 perf 收集程序运行信息并解析，完成编译阶段和二进制阶段反馈优化，提升 MySQL 数据库等主流应用场景的性能。
- 支持兆芯 KH-30000、KH-40000 处理器硬件架构特性。

- 修复龙芯架构动态库打包路径与系统不匹配问题。
- aarch64 架构下支持双精度浮点除法优化，提高除法操作执行效率。
- x86_64 架构下支持访存控制优化，提升 stream 性能。
- 支持海光 dhyana 和 dharma 处理器微架构特性。

5.10.2 llvm：编译器框架系统

LLVM 是一个开源的编译器基础设施项目，它提供了一种现代化的、可扩展的框架，用于构建编译器、优化器和代码生成器，支持多种编程语言和目标平台。

- LLVM 版本升级至 17.0.6，新增 loongarch64 架构 lp64s ABI 支持，添加 LSX, LASX, LVZ and LBT 指令集扩展支持。
- 支持命名参数。参数可以采用以下形式指定 name=value。
- 支持 X86_64 后端 SHA512、SM3、SM4 及 AVX-VNNI-INT16 指令集。
- 改进 LLVM IR，使用标准向量类型提高 LLVM IR 的通用性和性能优化能力。
- 支持 aarch64 架构 128 位原子操作，提高处理效率，充分利用流水线。
- 支持 aarch64 架构使用 SVE 进行复数自动矢量化，在支持 SVE 指令的机器上启用此优化后能够提升程序运行的性能。
- 新增 AMD GPU 后端以及其他各种改进。

5.10.3 binuils：二进制工具集

binutils 包括链接器、汇编器及一系列二进制工具，如 addr2line、ar、gprof、nm、objcopy、objdump、strip 等。

- binutils 升级至 2.41，新增 loongarch64 架构指令集：LSX、LASX、LVZ、LBT，并优化了链接器。
- 新增了对 Intel FRED、LKGS、AMX-COMPLEX 指令集的支持。
- 新增 aarch64 架构 SME2 的支持。
- 新增对 sw64 架构的支持。

- 新增对 zhaoxin 的 GMI 指令集的支持。

5.11 自研软件

5.11.1 网络故障分析技术

kynetobser 是一个适用于集群环境的网络故障分析技术，分为信息收集工具和聚合式分析工具。信息收集工具利用 ebpf 技术收集被监控节点的流量信息，聚合式分析工具负责汇总、匹配、计算报文延迟和丢包情况。

- 信息收集工具利用 ebpf 技术分别收集被监控节点协议栈各层流量信息。
  - 包括内核协议栈 2~4 层和应用层流量信息；
  - 可以通过参数指定收集特定层次的流量信息；
  - 信息以 json 格式保存，便于阅读和分析处理。
- 聚合式分析工具负责将各节点收集的信息进行统一分析。
  - 推算出协议栈各层次延迟；
  - 推算出收发节点之间网络链路延迟；
  - 统计丢包情况；
  - 终端显示收发节点之间及节点内部各层协议栈之间的报文延迟情况。

5.11.2 kylin-sysassist：麒麟智能运维助手

麒麟智能运维助手工具，支持日志收集、系统体检、系统监控及故障诊断四大功能，降低运维人员的技术门槛，提高了日志收集的效率与精准率；可以及时发现并修复系统存在的已知缺陷和漏洞及不合理配置，提高系统稳定性与安全性；可以有效的挖掘偶发故障的根因，补齐传统调试工具在偶发故障发生后无法收集有效信息的短板，并对常见的进程及网络故障问题进行智能化分析。支持如下特性：

- 一键收集全量日志或选择性日志：kylin-sysassist 支持用户一键收集全量日志或选择性收集指定日志，降低了运维人员的技术门槛，提高了日志收集的效率。
- 一键系统体检：kylin-sysassist 支持用户一键进行系统体检，可以有效的检测出

系统已知的缺陷和漏洞，并给出对应的修复方案；可以一键检查系统关键服务状态、内核调试参数等系统关键性配置，并对不合理的配置给出合理性建议。

- 系统监控：kylin-sysassist 支持进程、内存、存储、网络实时监控；可以监控指定进程的内存及 CPU 波动、进程状态、进程信号及进程数线程数；可以监控系统内存泄漏、内存回收；可以监控系统文件句柄及磁盘 inode 的使用情况；可以监控网络数据包。

- 故障诊断：kylin-sysassist 支持对系统监控中的进程监控及网络监控数据进行自动化分析，可以有效分析出进程内存占用和函数调用栈耗时情况；可以有效分析出网络丢包、延时和 IP 地址转换等问题。

5.11.3 授权激活工具集合

银河麒麟系统授权激活相关功能，用于授权商业版操作系统级服务，激活后的系统将提供长期功能更新及维护支持。麒麟授权系列组件包括 kylin-activation、libkylin-activation、librockey 和 kylin-activation-ukey-driver。它们作为授权功能的一部分，分别承担不同的任务。其中 kylin-activation 主要负责图形界面授权；libkylin-activation 提供命令行授权及底层校验库；librockey 和 kylin-activation-ukey-driver 分别为不同厂家提供的 UKEY 驱动程序，用于 UKEY 授权时识别和读写 UKEY。

- 授权包升级到 3.0，授权代码全面优化，通过了 fortify、sonarqube 扫描及渗透测试，全面提升了授权功能的安全性和稳定性。

- 添加了全架构授权类型区分功能，避免与桌面等授权文件混用。

- 修复了内存未释放问题，避免额外占用系统内存。

- 修复了 kms 授权采用广播模式激活时，小概率激活失败问题。

- 修复了 kms 授权私有化模式下，无法手动延期问题。

- 修复了 kms 授权服务端，批量取消激活成功后，几分钟后 web 界面恢复已激活状态问题。

- 修复了 kms 注册码小概率获取不准确，造成额外消耗激活点数问题。

- 修复图形界面 UKEY 授权错误提示不准确问题。
- 修复 kms 授权断网重连失败问题。
- 修复激活相关 dbus 接口 cve。
- 添加单元测试用，修复 fortify 扫描报错，优化代码，增强代码健壮性。
- 新增产品密钥激活功能。
- 新增定时更新平台授权状态到本地功能。
- 新增客户端取消激活功能。
- 新增跨产品架构授权激活功能。
- 新增 UKEY 授权中 UKEY 授权信息密文同步导出功能。
- 新增授权 LICENSE 加密备份功能。
- 新增授权激活兼容订阅功能。
- 新增 kms2.5 通信支持。
- 新增增值产品授权底层 API 激活接口。

5.11.4 kylin-pkgchecker：系统兼容性分析工具

银河麒麟系统兼容性分析工具（kylin-pkgchecker）能够在 x86_64、aarch64、loongarch64 架构下主要提供三项功能：系统兼容性分析，系统兼容性数据库生成，应用软件包兼容性分析。工具为系统间兼容性对比、系统升级、应用跨系统移植等场景中提供接口级粒度的兼容性风险检测能力，为应用生态适配提供不兼容接口数据指导。工具主要特性包括：

- 支持 x86_64/aarch64/loongarch64 架构下软件包兼容性分析。
- 支持命令行使用方式，提供一级参数 repo 实现系统兼容性分析、一级参数 data 实现系统动态库差异数据生成、一级参数 app 实现应用软件兼容性分析等功能。
- 系统兼容性分析功能支持对同一架构下不同版本系统仓库及系统镜像的兼容性检查，包括软件包兼容性等级、版本信息、依赖差异、命令差异、服务差异、配置差

异、二进制接口(ABI)差异，C 程序应用程序编程接口(API)等维度的检查，提供 html 可视化报告以及应用程序编程接口差异数据 csv 格式文件报告。

● 系统动态库差异数据库生成功能支持对比不同系统仓库的同名软件包中动态库接口差异信息并存储数据库。

● 应用软件兼容性分析功能支持对应用程序在不同系统版本间依赖关系及使用接口变更的差异数据分析，提供 html 可视化报告。

● 应用软件兼容性分析功能支持对当前系统环境的命令接口、板卡信息、设备驱动接口、内核选项参数、内核启动参数、端口、网络状态、进程、服务状态、系统调用接口、系统配置参数、环境变量，等 12 类系统环境信息收集，提供 html 可视化报告。

● 支持对本地同一架构的同名软件包不同版本间的兼容性扫描对比，输出 html 可视化报告。

5.11.5 kylin-warm: 热补丁制作和管理工具

热补丁是不需要重启操作系统、可以动态完成内核与关键应用服务的安全漏洞等问题修复的技术。kylin-warm 是为麒麟服务器操作系统量身定制的热补丁制作和激活管理工具。使用 kylin-warm 的热补丁制作功能可以生成热补丁安装包，包格式为 rpm。用 rpm 等命令安装热补丁以后，kylin-warm 服务程序可以自动侦测到。kylin-warm 管理工具支持热补丁的：加载、激活、去激活、卸载、查询、检查、保存、恢复。kylin-warm 自研特性功能主要包括：

● 以标准化的配置文件作为热补丁制作条件唯一输入口，解决目标程序版本数量大、CVE 漏洞多所带来的工程管理和质量管控难题。

● 构建自动存档功能，对质量检查回溯和二次制作形成有效支撑。

● 热补丁检查功能，包括一致性检查、校验合法性检查、模块依赖检查、符号冲突检查；新增加内核模块被替换检查功能。

● 健全的内核模块热补丁支持，包括热补丁安装和热补丁运行两个阶段的内核模块依赖检查。

● 热补丁顺序机制管理子系统，实现了状态切换顺序控制逻辑，在热补丁安装、激活、去激活、移除阶段引入热补丁顺序机制，以确保热补丁的管理和应用不增加系统安全风险，提高热补丁管理的准确性、可靠性和安全性。

● 支持 aarch64、x86_64、loongarch64 三个架构的 6.6 内核的热补丁制作和激活部署。

● 支持 aarch64、x86_64 两个架构的 glibc、qemu、openssl 的热补丁制作和激活部署。

5.11.6 extuner：应用场景调优工具

Extuner 是一款面向 Linux 平台的轻量级应用场景调优工具，集成系统全量数据采集、瓶颈信息分析、静态调优指导、动态智能调优、脱敏调优的功能。旨在辅助用户全面地分析系统性能瓶颈，充分发挥系统性能。

● 支持全量采集系统配置信息及实时指标信息，涵盖 CPU、内存、磁盘、网络、系统日志、热点数据采集等资源的运行情况。

● 支持对系统全量数据进行分析瓶颈信息，输出针对性的优化建议和操作指导。

● 提供简洁美观的 html 报告展示系统全量性能数据和关键瓶颈指标。

● 提供对大数据、数据库、中间件、web 等场景的专家调优参数指导，并提供一键式配置下发功能。

● 支持智能调优功能，通过 AI 算法对当前场景进行拟合函数分析，推理得出该场景的最佳参数配置组合。

● 支持对优化文件进行安全加密、混淆，保证核心优化技术方案不被泄露。

● 支持一键下发加密/混淆后的优化文件，简化调优操作过程。

5.11.7 exmonitor：应用性能监控工具

Exmonitor 应用性能监控软件，通过实时监控应用程序的性能指标和系统资源、进程、网络及磁盘状况等，形成了一个全方位、多层次的监控工具，极大地简化了系统管理员的问题排查与解决流程，为其提供了强有力的技术支持，能更加轻松、准确地

应对应用性能问题。

● 支持实时监控应用性能指标，精准捕捉性能异常。对用户设定的应用性能指标进行实时监控，及时发现并记录应用性能异常，管理员能够迅速获得应用性能的异常信息，从而及时响应并采取措施，防止问题扩大化。

● 支持实时监控多维度的系统资源，包括 CPU 和内存使用率、进程（进程状态、进程数和僵尸进程数）、网络（网卡带宽、网卡使用率）、磁盘（磁盘分区使用、inode 使用和磁盘时延）等，及时发现并记录异常监控数据，为应用性能问题分析提供了详尽的系统异常信息支持。

● 扩展支持应用和系统监控联动功能，即在监控到应用性能指标异常时，同步实时获取系统监控异常信息，综合两部分内容，形成最终监控结果。使得管理员在判断及分析应用性能问题时无需在多个监控工具间切换，通过 exmonitor 就能够获得全面、综合的异常信息，能更准确地诊断问题根源。

5.11.8 kylin-iodiag-tools：存储 IO 诊断工具

存储 IO 诊断工具是一款包含目录监控和进程监控两大功能的自研组件。它通过 ebpf 监控文件的系统调用和块层数据，实时输出详细的 IO 操作信息，如时间、进程名、PID、读写数据量和文件路径，帮助运维人员快速检测和定位操作系统 IO 的故障、性能问题。

● 支持监控指定目录或进程所有文件的元数据操作，获取创建、删除、打开、关闭、重命名等操作进程的进程名、pid、ppid、inode 号信息。

● 支持监控指定目录或进程的块层 IO 信息，包含 IO 操作文件的路径、到达 IO 观测点的时间、进程名、pid、ppid、操作类型、IO 大小、inode 号、扇区位置以及 IO 数据写入策略。

● 支持 IO 信息实时打印或日志归档。

● 支持统计指定进程的数据活跃度信息，包含读写文件分布的目录，磁盘及读写数据量。

5.11.9 kylin-fs-safe：文件系统元数据监控

文件系统元数据监控是一款用于 iSCSI 场景下的磁盘写入监控的自研组件。它通过 ebpf 监控文件系统层和块层数据，对可能破坏指定文件系统关键元数据的文件系统事件进行告警，记录事件类型、事件发生时间、事件所涉磁盘位置、发起事件的进程名及 ID、内核调用栈，运维人员可基于此信息快速发现并定位对文件系统元数据的破坏行为。

- 支持 XFS 和 EXT4 文件系统。
- 支持基于 iSCSI 设备的 partition 设备和 linear、multipath 两种类型的 dm 设备。
- 支持监控文件系统挂载事件、直接写入事件和针对块设备的缓存写入。
- 支持记录事件类型、事件发生时间、事件所涉磁盘位置、发起事件的进程名及 ID、内核调用栈。
- 支持同步告警信息至 syslog。

5.11.10 kyupgrade: 系统升级工具

Kyupgrade 工具实现了操作系统在不重新部署业务应用的情况下进行系统原地升级，支持 x86_64、aarch64 平台银河麒麟 V10 SP1、V10 SP2 、V10 SP3 2303 以及 V10 SP3 2403 系统原地升级到 V11 2503，主要特性包括：

- 支持 x86_64、aarch64 的 V10 SPx 系统原地平滑升级到 V11 2503，应用无需重新部署。
- 支持重复评估功能。在一次评估后如存在需要修改的系统配置，支持在修改配置后重复多次进行评估。
- 支持应用软件兼容性评估和第三方软件兼容性评估功能。实现在原地升级过程中，对应用软件兼容性与第三方软件兼容性影响的识别与告警。
- 支持白名单功能。提供保留原系统软件包版本不进行替换的配置文件。
- 支持提供评估报告和迁移报告。为原地升级过程中原系统基础信息，软件包替换信息等内容提供便利的可视化报告。

● 支持备份和还原功能。实现在原地升级过程中，对原系统全量级的备份。以及在升级后的回退还原功能。

● 支持内核参数配置同步功能，可选择将原系统的 sysctl 配置同步到升级后的 V11 2503 系统上。

● 支持系统升级后自检和信息对比功能。实现在完成原地升级之后，对升级后系统基础功能的自动检测，以及 V11 2503 和 V10 系统的信息对比。

5.11.11 ketones：内核观察工具

Ketones 是一个强大的 eBPF 程序集，旨在帮助用户在各架构操作系统环境中运行程序。与 BCC 工具集无缝兼容，可以轻松迁移和使用 ketones 而不会受到任何影响，并通过自研工具提供了更多观察内核的功能。

支持应用，系统库，系统调用，VFS，sockets，调度器，文件系统，网络协议栈，Volume Manager，虚拟内存，块设备，设备驱动，CPU 等各个子系统的信息获取和问题排查，以及优化方向指导。

5.11.12 kyldop：限定域优化工具

Kyldop 一款用于性能调优场景下的优化方案动态实施的自研工具。它通过 netlink 监控进程的创建和销毁，借此精确判断进程的生命周期，并根据进程运行状态动态调整优化方案，提高多进程应用场景下的整体性能，并减少优化方案对目标进程以外的不利影响。

● 支持 netlink 触发和轮询的进程监控方式。

● 支持使用国密算法对优化方案进行加密。

● 支持优化方案的无损回滚机制。

● 支持环境变量、服务状态、sysctl 参数等可变配置的调整。

5.11.13 kylin-subscription：订阅客户端工具

订阅客户端是一个基于命令行的工具，支持在线场景下客户将设备注册到远程服务器中，并管理设备的订阅信息。

- 允许设备注册。
- 支持查询设备的订阅状态和订阅产品。
- 允许切换设备，已订阅设备取消注册后即可释放订阅点数。
- 允许跨版本使用。
- 支持仓库访问。

5.11.14 kycompatguard：应用软件兼容性守护工具

Kycompatguard 是应用软件兼容性守护命令行工具和 dnf/yum 兼容性守护插件，提供对未安装应用软件程序包的兼容性分析功能，对已安装应用软件的兼容性分析功能和守护功能，确保通过 dnf/yum 对系统环境的变更不会影响已守护应用软件的兼容性，工具主要特性包括：

- 支持 x86_64/aarch64/loongarch64 架构下应用软件兼容性分析。
- 支持命令行使用方式，提供一级参数 check 实现应用软件兼容性分析、一级参数 remove 实对已守护应用软件的删除操作。
- 应用软件兼容性守护工具支持对 rpm、tar.gz、zip、tar 格式的程序包进行兼容性分析，支持对目录形式的已安装程序进行兼容性分析及保障。
- 兼容性守护工具可无缝集成到 dnf/yum 包管理工具组件中，通过指定 dnf/yum 命令行参数--compcheck 或在/etc/yum.conf 配置文件设置启用 compcheck=True 来确保兼容性保障能力的开启,并在命令执行过程中自动分析预变更包对已守护应用的兼容性是否有影响。
- 工具支持对用户手动编译、安装的系统组件引起的已守护应用的兼容性变更进行纠错处理，确保已守护应用的兼容性状态符合当前系统环境的现状。

5.11.15 kyCopilot：AI 应用工具

AI 应用工具 kyCopilot，通过调用大模型及使用 RAG 技术，实现了自然语言问答与辅助编程功能，并且能够通过自然语言触发调用调优工具进行场景优化。从而显著提升用户在麒麟操作系统上的工作效率，并大幅降低使用难度。

● 支持自然语言问答功能，具备辅助编程能力，包括代码生成、代码解析、单元测试用例生成及脚本生成等功能。

● 引入 RAG，支持麒麟知识问答功能及 deepseek-r1-7B 模型调用，提高了问答的准确性。

● 支持自然语言调用调优工具，具备系统指标采集和性能分析能力。

● 支持 shell 端或通过 VSCode 插件加载使用，提升了易用性。

● 支持本地化部署与敏感信息过滤功能，确保问答环境的安全，有效保护用户隐私。

● 支持 CPU 环境下运行，兼容 x86_64 与 aarch64 架构，不完全依赖 GPU，实现轻量化安装与使用，有效降低了用户的运行成本。

6 已知问题

6.1 架构与硬件支持

以下板卡因为厂商硬件不支持，所以只支持部分架构：

硬件类型	硬件厂商	支持架构
网卡	裕太微	x86_64、aarch64
网卡	北中网芯	x86_64、aarch64
网卡	众星微	x86_64、aarch64
网卡	楠菲	x86_64、aarch64
网卡	麦洛斯	x86_64、aarch64
网卡	云芯智联	x86_64、aarch64（不支持飞腾）
网卡	云脉芯联	x86_64、aarch64
网卡	大普威	x86_64、aarch64

网卡	星云智联	x86_64、aarch64
网卡	雄立	x86_64、aarch64
无线网卡	瑞昱	x86_64、aarch64
阵列卡	众星微	x86_64
阵列卡	华为鲲鹏	x86_64、aarch64
阵列卡	云芯智联	x86_64、aarch64
显卡	AMD	x86_64、aarch64
显卡	景嘉微	aarch64
显卡	凌久微（709）	aarch64
HBA	众星微	x86_64

6.2 内核

- 因为龙芯架构内核 4.19 和 6.6 中断控制器仿真模型不一样，导致 V10（带有 4.19 内核）Host 启动 V11 （6.6 内核）虚拟机会有问题，目前龙芯还没有这方面的解决方案。

- 内核合入飞腾推送的新 pmu 驱动补丁，其中包括了 ddr pmu 的改动，若服务器内存未插满会导致无法启动或者异常重启。需要升级固件 pbf 到 1.20 以上，或者在内核升级的时候屏蔽内核中的 phytium_ddr_pmu 驱动（加进 blacklist），在启动内核的时候识别黑名单禁止驱动加载。

- 海光处理器漏洞扫描，cat /sys/devices/system/cpu/vulnerabilities/* 输出结果存在 Vulnerable 字段，正在同海光处理。

- 因为 sched_ext、dm_vdo 未在龙芯适配，暂不支持。

- 因为 etmem 龙芯自身内核不支持，未使能。

- Ltp 测试 NUMA 架构支持性，飞腾和龙芯物理机偶现失败项，暂未解决。

- 龙芯处理器 blktests 测试 nvme 设备存在失败项 033~037，暂未解决。
- 添加壁纸管控，添加成功，后续 xorg 崩溃，暂未解决。
- 鲁棒性误操作测试存在失败子项，暂未解决。
- Arm 和龙芯处理器设置显示器方向失败，暂未解决。

6.3 核外软件

- GB18030 一号修改单支持正在进行，发布时对一号修改单的支持不完全。
- 龙芯无法使用网络安装虚拟机、龙芯不支持 cloud-hypervisor、不支持虚拟机配置 cpu 模式 host-passthrough 与 host-model。
- ARM 架构虚拟机暂不支持配置 QXL 显卡。
- 由于龙芯新旧世界系统调用有区别，因此 V10 龙芯相关的容器镜像在 V11 2503 龙芯架构上存在兼容性问题。
- 虚拟化组件中，cloud-hypervisor 暂无法在 ARM 架构下支持 vcpu 热插拔；
- 容器组件中，rubik 功耗管理功能只支持 intel 三代以上 cpu；rubik 的访存带宽和 LLC 限制功能需要 intel/海光 7480 RDT 或 鲲鹏 920 mpam 支持。
- 存储组件中，vdo 组件目前因内核 dm-vdo 模块对龙芯支持存在问题，所以暂时不支持龙芯架构；etmem 组件由于龙芯上缺少 etmem_swap 和 etmem_scan 内核模块，暂不支持龙芯架构；3fs 组件支持鲲鹏、海光、飞腾、intel 四架构，不支持龙芯架构。
- 编译工具链中，llvm-bolt 暂不支持龙芯架构二进制文件的调优。
- 安全组件中，因飞天诚信 UKEY 驱动未完成龙芯架构适配，多因子认证功能不支持龙芯架构；因 dim 未适配龙芯架构，dim 功能不支持龙芯架构。
- 网络组件中，kynetobser 基于 ebpf 技术开发，但是龙芯对 ebpf 支持不完善，所以 kynetobser 不支持龙芯架构。

6.4 自研软件

● kylin-sysassist：系统监控部分功能（内存泄露、内存回收、文件、进程信号、进程状态、网络监控）是基于 ebpf 技术开发，由于龙芯对 ebpf 支持不完善，所以系统监控部分功能不支持龙芯架构。

● 授权激活工具：UKEY 依赖不同架构的驱动，海泰方圆不支持龙芯架构。

● kylin-warm：应用服务热补丁不支持龙芯架构。

● Extuner：其中有部分功能依赖 ebpf 技术，由于 ebpf 技术对龙芯架构支持不完善，所以导致部分功能不支持龙芯架构。

● kyCopilot：由于依赖的 ollama 不支持龙芯，所以 kyCopilot 不支持龙芯架构。

● Ketones：龙芯架构暂未支持 trampoline，会有使得依赖该方式 hook 的工具无法使用。

● kylin-iodiag-tools：kylin-iodiag-tools 基于 ebpf 技术开发，但是龙芯对 ebpf 支持不完善，所以不支持龙芯架构；对指定目录进行监控时，基于 inode 号和挂载点作为唯一判断条件，所以不支持挂载点目录监控。

● kylin-fs-safe ：kylin-fs-safe 基于 ebpf 开发，由于龙芯对 ebpf 的支持不完善，kylin-fs-safe 暂不支持龙芯架构;所监控的块设备需基于 SCSI 协议的块设备，且该 SCSI 设备应有 naa.格式的 WWID。

7 漏洞修复

以下为银河麒麟高级服务器操作系统 V11 2503 中修复的 CVE 清单：

软件名称	修复CVE列表
389-ds-base	CVE-2020-35518 CVE-2021-3514 CVE-2021-3652 CVE-2024-1062
GraphicsMagick	CVE-2018-18544 CVE-2019-11005 CVE-2019-11006 CVE-2019-11007 CVE-2019-11008 CVE-2019-11009 CVE-2019-11010 CVE-2019-11473 CVE-2019-11474 CVE-2019-11505

	CVE-2019-11506 CVE-2019-12921 CVE-2019-7397 CVE-2020-10938 CVE-2020-12672 CVE-2022-1270
HikariCP	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105
ImageMagick	CVE-2022-1114 CVE-2022-1115 CVE-2022-2719 CVE-2022-3213 CVE-2022-32547 CVE-2022-44267 CVE-2022-44268 CVE-2023-1289 CVE-2023-1906 CVE-2023-34151 CVE-2023-34153 CVE-2023-3428 CVE-2023-5341
LibRaw	CVE-2018-20363 CVE-2018-20364 CVE-2018-20365 CVE-2023-1729 CVE-2025-43961 CVE-2025-43962 CVE-2025-43963 CVE-2025-43964
NetworkManager	CVE-2024-6501
NetworkManager-libreswan	CVE-2024-9050
OpenEXR	CVE-2021-20299 CVE-2021-20303 CVE-2021-3605 CVE-2022-45942 CVE-2023-5841 CVE-2024-31047
OpenIPMI	CVE-2024-42934
PackageKit	CVE-2020-16121
SDL	CVE-2019-13616
SDL2	CVE-2020-14409 CVE-2020-14410 CVE-2021-33657 CVE-2022-4743
abseil-cpp	CVE-2025-0838
aide	CVE-2021-45417
amanda	CVE-2022-37704 CVE-2022-37705 CVE-2023-30577
ansible	CVE-2020-1736 CVE-2020-1738 CVE-2024-0690 CVE-2024-8775 CVE-2024-9902
ant	CVE-2020-11979 CVE-2021-36373 CVE-2021-36374

aom	CVE-2024-5171
apache-commons-compress	CVE-2019-12402
apache-commons-fileupload	CVE-2023-24998
apache-commons-io	CVE-2021-29425 CVE-2024-47554
apache-mime4j	CVE-2024-21742
apache-mina	CVE-2019-0231 CVE-2021-41973
apache-poi	CVE-2019-12415
apache-sshd	CVE-2021-30129 CVE-2022-45047 CVE-2023-35887 CVE-2023-48795
apr	CVE-2017-12613 CVE-2022-24963 CVE-2023-49582
apr-util	CVE-2022-25147
aspell	CVE-2019-17544 CVE-2019-20433 CVE-2019-25051
assimp	CVE-2024-40724 CVE-2024-45679 CVE-2024-48423 CVE-2024-48424 CVE-2024-48425 CVE-2024-53425 CVE-2025-2151 CVE-2025-3015
atril	CVE-2023-51698 CVE-2023-52076
atune-collector	CVE-2024-24897
audiofile	CVE-2017-6828 CVE-2017-6829 CVE-2017-6831 CVE-2017-6838 CVE-2017-6839
augeas	CVE-2025-2588
avahi	CVE-2023-1981 CVE-2023-38469 CVE-2023-38470 CVE-2023-38471 CVE-2023-38472 CVE-2023-38473
avalon-framework	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105

avalon-logkit	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105
babel	CVE-2021-20095
batik	CVE-2019-17566 CVE-2020-11987 CVE-2022-38398 CVE-2022-38648 CVE-2022-40146 CVE-2022-41704 CVE-2022-42890 CVE-2022-44729 CVE-2022-44730
bcc	CVE-2024-2314
bcel	CVE-2022-34169
bind	CVE-2023-2911 CVE-2023-3341 CVE-2023-4408 CVE-2023-50387 CVE-2023-50868 CVE-2023-5517 CVE-2023-5679 CVE-2024-0760 CVE-2024-1737 CVE-2024-1975 CVE-2024-4076
binutils	CVE-2024-57360 CVE-2025-0840
bluez	CVE-2021-0129 CVE-2021-41229 CVE-2022-0204 CVE-2022-39176 CVE-2022-39177 CVE-2023-27349 CVE-2023-45866 CVE-2023-50229 CVE-2023-50230
booth	CVE-2024-3049
botan2	CVE-2022-43705 CVE-2024-34702 CVE-2024-34703 CVE-2024-39312 CVE-2024-50382
bouncycastle	CVE-2019-17359 CVE-2020-15522 CVE-2023-33201
brotli	CVE-2020-8927
bubblewrap	CVE-2024-42472
buildah	CVE-2024-1753 CVE-2024-24786 CVE-2024-28180
busybox	CVE-2022-48174 CVE-2023-42363 CVE-2023-42364 CVE-2023-42365 CVE-2023-42366
byacc	CVE-2021-33641 CVE-2021-33642
c-ares	CVE-2021-3672 CVE-2022-4904 CVE-2023-31124 CVE-2023-31130 CVE-2023-31147 CVE-2023-32067 CVE-2024-25629

cairo	CVE-2019-6461 CVE-2019-6462 CVE-2020-35492
ceph	CVE-2023-46159
cfitsio	CVE-2018-3848 CVE-2018-3849
chrony	CVE-2020-14367
cifs-utils	CVE-2021-20208
cjose	CVE-2023-37464
cjson	CVE-2023-50471 CVE-2023-50472 CVE-2024-31755
clamav	CVE-2022-20698 CVE-2022-20770 CVE-2022-20771 CVE-2022-20785 CVE-2022-20792 CVE-2023-20032 CVE-2023-20052 CVE-2023-20197
cockpit	CVE-2021-3660 CVE-2024-6126
colord	CVE-2021-42523
compat-icu	CVE-2020-10531 CVE-2020-21913
compat-openssl11	CVE-2023-5678 CVE-2024-0727 CVE-2024-13176 CVE-2024-2511 CVE-2024-4741 CVE-2024-5535 CVE-2024-9143
compat-protobuf	CVE-2021-22570 CVE-2022-1941 CVE-2022-3171
containernetworking-plugins	CVE-2023-24534 CVE-2023-24536 CVE-2023-24537 CVE-2023-24538
cpio	CVE-2015-1197 CVE-2021-38185
cpp-httplib	CVE-2023-26130
cri-tools	CVE-2024-24786
crun	CVE-2022-27650 CVE-2025-24965
cryptacular	CVE-2020-7226

ctags	CVE-2022-4515
cups	CVE-2023-34241 CVE-2023-4504 CVE-2024-35235 CVE-2024-47175
cups-filters	CVE-2023-24805 CVE-2024-47076 CVE-2024-47175 CVE-2024-47176 CVE-2024-47850
curl	CVE-2024-11053 CVE-2024-7264 CVE-2024-8096 CVE-2024-9681 CVE-2025-0167 CVE-2025-0725
cyrus-sasl	CVE-2022-24407
datanucleus-api-jdo	CVE-2021-44228 CVE-2021-45105
datanucleus-core	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105
datanucleus-rdbms	CVE-2021-44228 CVE-2021-45105
dbus	CVE-2022-42010 CVE-2022-42011 CVE-2022-42012 CVE-2023-34969
deltarpm	CVE-2005-1849 CVE-2016-9840 CVE-2016-9841 CVE-2016-9843 CVE-2018-25032 CVE-2022-37434
derby	CVE-2018-1313 CVE-2023-48284
dhcp	CVE-2022-2795 CVE-2022-38177 CVE-2022-38178 CVE-2023-3341 CVE-2024-11187 CVE-2024-1737 CVE-2024-1975
djvulibre	CVE-2019-15142 CVE-2019-15143 CVE-2019-15144 CVE-2019-15145 CVE-2019-18804 CVE-2021-32490 CVE-2021-32491 CVE-2021-32492 CVE-2021-32493 CVE-2021-3500 CVE-2021-3630 CVE-2021-46310 CVE-2021-46312
dmidecode	CVE-2023-30630
dnsjava	CVE-2024-25638
dnsmasq	CVE-2023-28450
dom4j	CVE-2020-10683

dovecot	CVE-2022-30550 CVE-2024-23184 CVE-2024-23185
dpdk	CVE-2024-11614
dpkg	CVE-2022-1664
eclipse	CVE-2020-27225
eclipse-ecf	CVE-2014-0363
ecryptfs-utils	CVE-2016-6224
edk2	CVE-2023-45236 CVE-2023-45237 CVE-2023-5363 CVE-2024-13176 CVE-2024-38797 CVE-2024-4741 CVE-2024-9143
elfutils	CVE-2024-25260 CVE-2025-1352 CVE-2025-1365 CVE-2025-1371 CVE-2025-1372 CVE-2025-1376 CVE-2025-1377
emacs	CVE-2022-45939 CVE-2022-48337 CVE-2022-48338 CVE-2022-48339 CVE-2023-27985 CVE-2023-27986 CVE-2023-28617 CVE-2024-30202 CVE-2024-30203 CVE-2024-30204 CVE-2024-30205 CVE-2024-39331 CVE-2025-1244
erlang	CVE-2023-48795
espeak-ng	CVE-2023-49990 CVE-2023-49994
etcd	CVE-2021-28235 CVE-2021-44716 CVE-2022-3064 CVE-2022-34038 CVE-2022-41723 CVE-2023-32082 CVE-2023-39325 CVE-2023-45288
exiv2	CVE-2021-29463 CVE-2021-29464 CVE-2021-29473 CVE-2021-29623 CVE-2021-32617 CVE-2022-3755 CVE-2022-3756 CVE-2023-44398 CVE-2024-24826 CVE-2024-25112 CVE-2024-39695
expat	CVE-2022-43680 CVE-2023-52425 CVE-2024-45490 CVE-2024-45491 CVE-2024-45492 CVE-2024-50602

f2fs-tools	CVE-2020-6104 CVE-2020-6105 CVE-2020-6106 CVE-2020-6107 CVE-2020-6108
festival	CVE-2010-3996
fetchmail	CVE-2021-39272
ffmpeg	CVE-2023-49501 CVE-2024-32228 CVE-2024-35365 CVE-2024-35366 CVE-2024-35367 CVE-2024-35368 CVE-2024-35369 CVE-2024-36613 CVE-2024-36616 CVE-2024-36617 CVE-2024-36618 CVE-2024-36619 CVE-2024-7055
flac	CVE-2020-0499 CVE-2021-0561
flatbuffers	CVE-2020-35864
flatpak	CVE-2019-8308 CVE-2021-41133 CVE-2021-43860 CVE-2022-21682 CVE-2023-28100 CVE-2023-28101 CVE-2024-32462 CVE-2024-42472
fluidsynth	CVE-2021-21417
fontforge	CVE-2024-25081 CVE-2024-25082
fonttools	CVE-2023-45139
fop	CVE-2024-28168
freeglut	CVE-2024-24258 CVE-2024-24259
freeimage	CVE-2020-21427 CVE-2020-21428 CVE-2020-22524 CVE-2020-24292 CVE-2020-24293 CVE-2020-24295 CVE-2021-33367 CVE-2021-40263 CVE-2021-40266 CVE-2023-47995 CVE-2023-47997
freeradius	CVE-2022-41859 CVE-2022-41860 CVE-2022-41861 CVE-2024-3596
freerdp	CVE-2022-39282 CVE-2022-39316 CVE-2022-39317 CVE-2022-39318 CVE-2022-39319 CVE-2022-39320 CVE-2022-39347 CVE-2022-41877 CVE-2024-22211 CVE-2024-32039 CVE-2024-32040 CVE-2024-32041 CVE-2024-32458 CVE-2024-32459 CVE-2024-32460

	CVE-2024-32658 CVE-2024-32659 CVE-2024-32660 CVE-2024-32661
freetds	CVE-2019-13508
freetype	CVE-2022-27454 CVE-2022-27455 CVE-2022-27456 CVE-2023-2004 CVE-2025-27363
fribidi	CVE-2019-18397 CVE-2022-25308 CVE-2022-25309 CVE-2022-25310
future	CVE-2022-40899
game-music-emu	CVE-2017-17446
ganglia	CVE-2019-20378 CVE-2019-20379
gd	CVE-2021-38115 CVE-2021-40145 CVE-2021-40812
gdb	CVE-2023-39128 CVE-2023-39129 CVE-2023-39130
gdk-pixbuf2	CVE-2022-48622
ghostscript	CVE-2024-29511 CVE-2024-33869 CVE-2024-46951 CVE-2024-46952 CVE-2024-46953 CVE-2024-46955 CVE-2024-46956 CVE-2025-27830 CVE-2025-27831 CVE-2025-27832 CVE-2025-27833 CVE-2025-27834 CVE-2025-27835 CVE-2025-27836
giflib	CVE-2021-40633 CVE-2022-28506 CVE-2023-39742 CVE-2023-48161
git	CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-50349 CVE-2024-52005 CVE-2024-52006
glib2	CVE-2024-34397 CVE-2024-52533 CVE-2025-3360
glibc	CVE-2025-0395
glusterfs	CVE-2023-26253
gmp	CVE-2021-43618
gnome-autoar	CVE-2020-36241 CVE-2021-28650
gnulib	CVE-2018-17942

gnupg2	CVE-2022-34903 CVE-2025-30258
gnutls	CVE-2023-5981 CVE-2024-0553 CVE-2024-0567 CVE-2024-12243 CVE-2024-28834 CVE-2024-28835
golang	CVE-2024-34155 CVE-2024-34156 CVE-2024-34158
google-gson	CVE-2022-25647
gradle	CVE-2019-16370
graphviz	CVE-2020-18032 CVE-2023-46045
grilo	CVE-2021-39365
groovy	CVE-2020-17521
grpc	CVE-2023-4785 CVE-2024-11407 CVE-2024-7246
grub2	CVE-2024-45774 CVE-2024-49504
gsl	CVE-2024-50610
gssntlmssp	CVE-2023-25563 CVE-2023-25564 CVE-2023-25565 CVE-2023-25567
gstreamer1-plugins-bad-free	CVE-2021-3185 CVE-2023-37329 CVE-2023-40474 CVE-2023-40475 CVE-2023-40476 CVE-2023-44446
gstreamer1-plugins-base	CVE-2024-47538 CVE-2024-47541 CVE-2024-47542 CVE-2024-47600 CVE-2024-47607 CVE-2024-47615 CVE-2024-47835
gstreamer1-plugins-good	CVE-2021-3497 CVE-2021-3498 CVE-2022-1920 CVE-2022-1925 CVE-2022-2122 CVE-2023-37327 CVE-2024-47537 CVE-2024-47539 CVE-2024-47540 CVE-2024-47543 CVE-2024-47544 CVE-2024-47545 CVE-2024-47546 CVE-2024-47596 CVE-2024-47597 CVE-2024-47598 CVE-2024-47599 CVE-2024-47601 CVE-2024-47602 CVE-2024-47603 CVE-2024-47606 CVE-2024-47613 CVE-2024-47774 CVE-2024-47775 CVE-2024-47776

	CVE-2024-47777 CVE-2024-47778 CVE-2024-47834
gtk2	CVE-2024-6655
gtk3	CVE-2024-6655
guava	CVE-2020-8908 CVE-2023-2976
guava20	CVE-2020-8908 CVE-2023-2976
gupnp	CVE-2021-33516
gzip	CVE-2022-1271
haproxy	CVE-2024-45506 CVE-2024-49214 CVE-2024-53008
harfbuzz	CVE-2022-33068 CVE-2023-25193
hdf5	CVE-2018-13867 CVE-2018-13871 CVE-2018-13875 CVE-2018-14031 CVE-2018-14034 CVE-2018-16438 CVE-2018-17433 CVE-2018-17436 CVE-2019-8396 CVE-2020-10809 CVE-2020-10812 CVE-2021-37501 CVE-2024-29157 CVE-2024-29158 CVE-2024-29159 CVE-2024-29160 CVE-2024-29161 CVE-2024-29162 CVE-2024-29163 CVE-2024-29164 CVE-2024-29165 CVE-2024-29166 CVE-2024-32605 CVE-2024-32606 CVE-2024-32607 CVE-2024-32608 CVE-2024-32609 CVE-2024-32610 CVE-2024-32611 CVE-2024-32612 CVE-2024-32613 CVE-2024-32614 CVE-2024-32615 CVE-2024-32616 CVE-2024-32617 CVE-2024-32618 CVE-2024-32619 CVE-2024-32620 CVE-2024-32621 CVE-2024-32622 CVE-2024-32623 CVE-2024-32624 CVE-2024-33873 CVE-2024-33874 CVE-2024-33875 CVE-2024-33876 CVE-2024-33877
hibernate	CVE-2019-14900 CVE-2020-25638
hibernate-validator	CVE-2017-7536 CVE-2019-10219 CVE-2020-10693
hibernate3	CVE-2019-14900 CVE-2020-25638

hibernate4	CVE-2019-14900 CVE-2020-25638
hiredis	CVE-2021-32765
hivex	CVE-2021-3504 CVE-2021-3622
hsqldb	CVE-2022-41853
hsqldb1	CVE-2022-41853
htslib	CVE-2020-36403
httpd	CVE-2023-31122 CVE-2023-38709 CVE-2023-43622 CVE-2023-45802 CVE-2024-24795 CVE-2024-27316 CVE-2024-36387 CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38476 CVE-2024-38477 CVE-2024-39573 CVE-2024-39884 CVE-2024-40725
hunspell	CVE-2019-16707
hwloc	CVE-2022-47022
indent	CVE-2023-40305 CVE-2024-0911
infinispan	CVE-2016-0750 CVE-2017-15089 CVE-2019-10174 CVE-2021-44228 CVE-2021-45105
iniparser	CVE-2023-33461 CVE-2025-0633
intel-sgx-ssl	CVE-2022-0778 CVE-2022-1292 CVE-2022-2068 CVE-2022-2097
iperf3	CVE-2023-38403 CVE-2024-26306
ipmitool	CVE-2011-4339
iptraf-ng	CVE-2024-52949
irssi	CVE-2019-13045
jackson	CVE-2019-10172
jackson-databind	CVE-2019-17531 CVE-2020-25649 CVE-2020-35490 CVE-2020-35491 CVE-2020-35728 CVE-2020-36179 CVE-2020-36180 CVE-2020-36181 CVE-2020-36182 CVE-2020-36183

	CVE-2020-36184 CVE-2020-36185 CVE-2020-36186 CVE-2020-36187 CVE-2020-36188 CVE-2020-36189 CVE-2020-36518 CVE-2021-20190 CVE-2022-42003 CVE-2022-42004
jackson-dataformats-binary	CVE-2020-28491
jasper	CVE-2018-18873 CVE-2018-19139 CVE-2018-19539 CVE-2018-19540 CVE-2018-19541 CVE-2018-20570 CVE-2018-20622 CVE-2018-9055 CVE-2018-9154 CVE-2018-9252 CVE-2021-27845 CVE-2023-51257 CVE-2024-31744
jbig2dec	CVE-2023-46361
jbigkit	CVE-2017-9937
jboss-logging	CVE-2021-44228 CVE-2021-45105
jdom2	CVE-2021-33813
jersey	CVE-2021-28168
jettison	CVE-2022-40149 CVE-2022-40150 CVE-2022-45685 CVE-2022-45693 CVE-2023-1436
jetty	CVE-2019-10241 CVE-2021-28169 CVE-2021-34428 CVE-2022-2047 CVE-2022-2048 CVE-2023-26048 CVE-2023-26049 CVE-2023-36479 CVE-2023-40167 CVE-2024-6762
jgit	CVE-2023-4759
jgroups	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105
jose	CVE-2023-50967
jruby	CVE-2023-28756
json-lib	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105 CVE-2024-47855
json-path	CVE-2023-51074
json-smart	CVE-2023-1370

jsoup	CVE-2022-36033
junit	CVE-2020-15250
keepalived	CVE-2021-44225
kernel（仅统计7分以上高危CVE）	CVE-2011-1180 CVE-2011-1771 CVE-2011-2525 CVE-2011-3359 CVE-2011-5327 CVE-2012-0044 CVE-2012-0207 CVE-2012-1097 CVE-2012-6701 CVE-2012-6703 CVE-2012-6704 CVE-2012-6712 CVE-2013-1943 CVE-2013-2094 CVE-2013-2897 CVE-2013-4588 CVE-2014-7826 CVE-2014-8160 CVE-2014-8369 CVE-2014-9322 CVE-2014-9803 CVE-2014-9904 CVE-2015-8962 CVE-2015-8963 CVE-2015-9004 CVE-2016-10044 CVE-2016-10142 CVE-2016-10153 CVE-2016-10200 CVE-2016-10229 CVE-2016-10764 CVE-2016-10905 CVE-2016-10907 CVE-2016-1575 CVE-2016-1576 CVE-2016-1583 CVE-2016-2069 CVE-2016-2070 CVE-2016-2117 CVE-2016-3070 CVE-2016-3134 CVE-2016-3135 CVE-2016-3157 CVE-2016-3672 CVE-2016-3713 CVE-2016-3841 CVE-2016-3955 CVE-2016-4470 CVE-2016-4485 CVE-2016-4557 CVE-2016-4558 CVE-2016-4565 CVE-2016-4580 CVE-2016-4794 CVE-2016-4805 CVE-2016-4951 CVE-2016-4998 CVE-2016-5195 CVE-2016-5244 CVE-2016-5829 CVE-2016-5863 CVE-2016-6187 CVE-2016-6787 CVE-2016-7039 CVE-2016-7117 CVE-2016-7425 CVE-2016-7911 CVE-2016-7912 CVE-2016-7913 CVE-2016-8399 CVE-2016-8632 CVE-2016-8636 CVE-2016-8655 CVE-2016-9083 CVE-2016-9120 CVE-2016-9313 CVE-2016-9644 CVE-2016-9754 CVE-2016-9755 CVE-2016-9793 CVE-2016-9794 CVE-2016-9806 CVE-2017-0786 CVE-2017-0861 CVE-2017-1000111 CVE-2017-1000112 CVE-2017-1000251 CVE-2017-1000363 CVE-2017-1000365 CVE-2017-1000371 CVE-2017-1000379 CVE-2017-10661 CVE-2017-16526 CVE-2017-18202

	CVE-2017-18222 CVE-2017-2634 CVE-2017-5123 CVE-2017-5546 CVE-2017-5547 CVE-2017-5548 CVE-2017-5576 CVE-2017-5897 CVE-2017-5972 CVE-2017-6001 CVE-2017-6074 CVE-2017-6214 CVE-2017-6280 CVE-2017-6345 CVE-2017-6346 CVE-2017-6347 CVE-2017-6874 CVE-2017-7184 CVE-2017-7187 CVE-2017-7277 CVE-2017-7294 CVE-2017-7308 CVE-2017-7374 CVE-2017-7477 CVE-2017-7482 CVE-2017-7487 CVE-2017-7518 CVE-2017-7533 CVE-2017-7541 CVE-2017-7618 CVE-2017-7645 CVE-2017-7889 CVE-2017-7895 CVE-2017-8064 CVE-2017-8068 CVE-2017-8070 CVE-2017-8240 CVE-2017-8241 CVE-2017-8797 CVE-2017-8824 CVE-2017-8890 CVE-2017-9074 CVE-2017-9075 CVE-2017-9076 CVE-2017-9077 CVE-2017-9725 CVE-2017-9984 CVE-2017-9985 CVE-2017-9986 CVE-2018-1000026 CVE-2018-1000028 CVE-2018-10675 CVE-2018-10853 CVE-2018-1087 CVE-2018-10878 CVE-2018-10901 CVE-2018-10902 CVE-2018-11506 CVE-2018-12233 CVE-2018-12714 CVE-2018-13405 CVE-2018-13406 CVE-2018-14619 CVE-2018-14633 CVE-2018-14634 CVE-2018-16882 CVE-2019-11478 CVE-2019-11479 CVE-2019-11487 CVE-2019-11811 CVE-2019-11815 CVE-2019-12454 CVE-2019-12456 CVE-2019-12881 CVE-2019-13272 CVE-2019-14814 CVE-2019-14815 CVE-2019-14816 CVE-2019-14821 CVE-2019-14835 CVE-2019-14895 CVE-2019-14896 CVE-2019-14897 CVE-2019-15117 CVE-2019-15505 CVE-2019-15916 CVE-2019-15918 CVE-2019-15926 CVE-2019-15927 CVE-2019-16413 CVE-2019-16746 CVE-2019-16995 CVE-2019-17075 CVE-2019-17133 CVE-2019-17666 CVE-2019-18675 CVE-2019-18683 CVE-2019-18805 CVE-2019-18810 CVE-2019-19050 CVE-2019-19052 CVE-2019-19060 CVE-2019-19061 CVE-2019-19070 CVE-2019-19071 CVE-2019-19074 CVE-2019-19075 CVE-2019-19377 CVE-2019-19447 CVE-2019-19448

	CVE-2019-19543 CVE-2019-19768 CVE-2019-2000 CVE-2019-2024 CVE-2019-20425 CVE-2019-6974 CVE-2019-9458 CVE-2019-9500 CVE-2019-9503 CVE-2019-9506 CVE-2020-0432 CVE-2020-0433 CVE-2020-0444 CVE-2020-0466 CVE-2020-11668 CVE-2020-12351 CVE-2020-12362 CVE-2020-12653 CVE-2020-12654 CVE-2020-12657 CVE-2020-14386 CVE-2020-27068 CVE-2020-36387 CVE-2020-8428 CVE-2021-0512 CVE-2021-1048 CVE-2021-20194 CVE-2021-20226 CVE-2021-20322 CVE-2021-22543 CVE-2021-22555 CVE-2021-22600 CVE-2021-23133 CVE-2021-26708 CVE-2021-26930 CVE-2021-27364 CVE-2021-27365 CVE-2021-28375 CVE-2021-28660 CVE-2021-28691 CVE-2021-29154 CVE-2021-29657 CVE-2021-32399 CVE-2021-33034 CVE-2021-33909 CVE-2021-3483 CVE-2021-34866 CVE-2021-3493 CVE-2021-34981 CVE-2021-3563 CVE-2021-3609 CVE-2021-3612 CVE-2021-3640 CVE-2021-3653 CVE-2021-3656 CVE-2021-3715 CVE-2021-3739 CVE-2021-3743 CVE-2021-3752 CVE-2021-38160 CVE-2021-38201 CVE-2021-38202 CVE-2021-38300 CVE-2021-39634 CVE-2021-39685 CVE-2021-39698 CVE-2021-39801 CVE-2021-4028 CVE-2021-4037 CVE-2021-40490 CVE-2021-4083 CVE-2021-41073 CVE-2021-4157 CVE-2021-41864 CVE-2021-42252 CVE-2021-45485 CVE-2021-46955 CVE-2021-47094 CVE-2021-47123 CVE-2021-47131 CVE-2021-47259 CVE-2021-47261 CVE-2021-47324 CVE-2021-47394 CVE-2021-47493 CVE-2021-47496 CVE-2021-47517 CVE-2021-47561 CVE-2022-1043 CVE-2022-1048 CVE-2022-23039 CVE-2022-23040 CVE-2022-23041 CVE-2022-23222 CVE-2022-24122 CVE-2022-24958 CVE-2022-25636 CVE-2022-2590 CVE-2022-26365 CVE-2022-2639 CVE-2022-26490 CVE-2022-27223 CVE-2022-28390 CVE-2022-29156 CVE-2022-2938 CVE-2022-29581 CVE-2022-29582 CVE-2022-2964 CVE-2022-2978 CVE-2022-29968

	CVE-2022-3028 CVE-2022-30594 CVE-2022-3170 CVE-2022-3176 CVE-2022-3202 CVE-2022-32250 CVE-2022-3239 CVE-2022-33740 CVE-2022-33741 CVE-2022-33742 CVE-2022-3424 CVE-2022-34918 CVE-2022-3564 CVE-2022-3565 CVE-2022-3566 CVE-2022-3625 CVE-2022-3635 CVE-2022-3640 CVE-2022-36946 CVE-2022-39189 CVE-2022-4095 CVE-2022-41674 CVE-2022-41858 CVE-2022-42719 CVE-2022-42720 CVE-2022-42896 CVE-2022-4379 CVE-2022-43945 CVE-2022-48791 CVE-2022-48837 CVE-2022-48851 CVE-2022-48866 CVE-2022-48925 CVE-2022-48948 CVE-2022-48951 CVE-2022-49763 CVE-2022-49789 CVE-2022-49807 CVE-2022-49813 CVE-2022-49840 CVE-2022-49863 CVE-2022-49876 CVE-2022-49899 CVE-2022-49910 CVE-2022-49917 CVE-2022-49932 CVE-2022-49934 CVE-2022-49935 CVE-2022-49937 CVE-2022-49942 CVE-2022-49944 CVE-2022-49947 CVE-2022-49951 CVE-2022-49960 CVE-2022-49962 CVE-2022-49964 CVE-2022-49969 CVE-2022-49970 CVE-2022-49972 CVE-2022-49977 CVE-2022-49980 CVE-2022-49985 CVE-2022-49986 CVE-2022-49987 CVE-2022-49989 CVE-2022-49991 CVE-2022-49993 CVE-2022-49994 CVE-2022-49998 CVE-2022-50000 CVE-2022-50001 CVE-2022-50002 CVE-2022-50003 CVE-2022-50004 CVE-2022-50008 CVE-2022-50011 CVE-2022-50014 CVE-2022-50015 CVE-2022-50016 CVE-2022-50020 CVE-2022-50021 CVE-2022-50022 CVE-2022-50028 CVE-2022-50030 CVE-2022-50031 CVE-2022-50035 CVE-2022-50039 CVE-2022-50040 CVE-2022-50044 CVE-2022-50049 CVE-2022-50050 CVE-2022-50051 CVE-2022-50053 CVE-2022-50054 CVE-2022-50055 CVE-2022-50056 CVE-2022-50057 CVE-2022-50058 CVE-2022-50063 CVE-2022-50064 CVE-2022-50066 CVE-2022-50068 CVE-2022-50070 CVE-2022-50072 CVE-2022-50073 CVE-2022-50075 CVE-2022-50079 CVE-2022-50083 CVE-2022-50087 CVE-2022-50093

	CVE-2022-50095 CVE-2022-50115 CVE-2022-50117 CVE-2022-50133 CVE-2022-50148 CVE-2022-50167 CVE-2022-50174 CVE-2022-50177 CVE-2022-50178 CVE-2022-50179 CVE-2022-50181 CVE-2022-50182 CVE-2022-50185 CVE-2022-50187 CVE-2022-50190 CVE-2022-50193 CVE-2022-50200 CVE-2022-50202 CVE-2022-50205 CVE-2022-50210 CVE-2022-50211 CVE-2022-50212 CVE-2022-50214 CVE-2022-50215 CVE-2022-50217 CVE-2022-50220 CVE-2022-50221 CVE-2022-50224 CVE-2022-50227 CVE-2022-50228 CVE-2022-50229 CVE-2023-1295 CVE-2023-1829 CVE-2023-2007 CVE-2023-25775 CVE-2023-26606 CVE-2023-28410 CVE-2023-28466 CVE-2023-3106 CVE-2023-3111 CVE-2023-3141 CVE-2023-32233 CVE-2023-32247 CVE-2023-32250 CVE-2023-32252 CVE-2023-32254 CVE-2023-32257 CVE-2023-32258 CVE-2023-32629 CVE-2023-3269 CVE-2023-3317 CVE-2023-34319 CVE-2023-3777 CVE-2023-42753 CVE-2023-45871 CVE-2023-46838 CVE-2023-51042 CVE-2023-51043 CVE-2023-51779 CVE-2023-51780 CVE-2023-51781 CVE-2023-52340 CVE-2023-52468 CVE-2023-52480 CVE-2023-52509 CVE-2023-52599 CVE-2023-52600 CVE-2023-52601 CVE-2023-52604 CVE-2023-52640 CVE-2023-52751 CVE-2023-52755 CVE-2023-52760 CVE-2023-52769 CVE-2023-52772 CVE-2023-52827 CVE-2023-52829 CVE-2023-52846 CVE-2023-52852 CVE-2023-52880 CVE-2023-52881 CVE-2023-52885 CVE-2023-53055 CVE-2023-53062 CVE-2023-53107 CVE-2023-53133 CVE-2023-53137 CVE-2023-5717 CVE-2023-6040 CVE-2023-6111 CVE-2023-6200 CVE-2023-6270 CVE-2023-6531 CVE-2023-6606 CVE-2023-6610 CVE-2023-6817 CVE-2023-6931 CVE-2023-6932 CVE-2024-0193 CVE-2024-0565 CVE-2024-0582 CVE-2024-0646 CVE-2024-0775 CVE-2024-1085 CVE-2024-1086 CVE-2024-1312 CVE-2024-25744 CVE-2024-26582 CVE-2024-26585 CVE-2024-26594

	CVE-2024-26598 CVE-2024-26610 CVE-2024-26630 CVE-2024-26652 CVE-2024-26665 CVE-2024-26668 CVE-2024-26669 CVE-2024-26692 CVE-2024-26766 CVE-2024-26852 CVE-2024-26865 CVE-2024-26921 CVE-2024-26923 CVE-2024-26929 CVE-2024-26930 CVE-2024-26939 CVE-2024-26996 CVE-2024-27043 CVE-2024-27050 CVE-2024-27398 CVE-2024-27399 CVE-2024-27413 CVE-2024-35803 CVE-2024-35817 CVE-2024-35861 CVE-2024-35862 CVE-2024-35863 CVE-2024-35864 CVE-2024-35867 CVE-2024-35948 CVE-2024-35949 CVE-2024-35950 CVE-2024-36013 CVE-2024-36477 CVE-2024-36899 CVE-2024-36904 CVE-2024-36921 CVE-2024-36964 CVE-2024-36971 CVE-2024-36974 CVE-2024-36979 CVE-2024-37353 CVE-2024-38541 CVE-2024-38559 CVE-2024-38560 CVE-2024-38583 CVE-2024-38610 CVE-2024-38664 CVE-2024-39277 CVE-2024-39291 CVE-2024-39463 CVE-2024-39479 CVE-2024-39480 CVE-2024-39494 CVE-2024-39495 CVE-2024-39496 CVE-2024-40899 CVE-2024-40902 CVE-2024-40903 CVE-2024-40909 CVE-2024-40910 CVE-2024-40937 CVE-2024-40954 CVE-2024-40956 CVE-2024-40989 CVE-2024-40994 CVE-2024-41003 CVE-2024-41011 CVE-2024-41057 CVE-2024-41058 CVE-2024-41059 CVE-2024-41062 CVE-2024-41069 CVE-2024-41087 CVE-2024-41090 CVE-2024-41092 CVE-2024-41096 CVE-2024-42072 CVE-2024-42145 CVE-2024-42154 CVE-2024-42159 CVE-2024-42160 CVE-2024-42161 CVE-2024-42162 CVE-2024-42224 CVE-2024-42225 CVE-2024-42228 CVE-2024-42271 CVE-2024-42284 CVE-2024-42285 CVE-2024-42301 CVE-2024-42302 CVE-2024-42313 CVE-2024-42314 CVE-2024-43858 CVE-2024-43861 CVE-2024-43882 CVE-2024-43883 CVE-2024-43888 CVE-2024-43900 CVE-2024-44934 CVE-2024-44938 CVE-2024-44940 CVE-2024-45026 CVE-2024-46673 CVE-2024-46687 CVE-2024-46740 CVE-2024-46741 CVE-2024-46743 CVE-2024-46746

	CVE-2024-46757 CVE-2024-46758 CVE-2024-46798 CVE-2024-46800 CVE-2024-46804 CVE-2024-46813 CVE-2024-46814 CVE-2024-46815 CVE-2024-46818 CVE-2024-46821 CVE-2024-46831 CVE-2024-46849 CVE-2024-46852 CVE-2024-46854 CVE-2024-46858 CVE-2024-46865 CVE-2024-47719 CVE-2024-47741 CVE-2024-47747 CVE-2024-47748 CVE-2024-49852 CVE-2024-49860 CVE-2024-49931 CVE-2024-49936 CVE-2024-49991 CVE-2024-50036 CVE-2024-50051 CVE-2024-50055 CVE-2024-50066 CVE-2024-50067 CVE-2024-50083 CVE-2024-50086 CVE-2024-50112 CVE-2024-50115 CVE-2024-50121 CVE-2024-50124 CVE-2024-50125 CVE-2024-50126 CVE-2024-50127 CVE-2024-50128 CVE-2024-50130 CVE-2024-50131 CVE-2024-50208 CVE-2024-50215 CVE-2024-50217 CVE-2024-50222 CVE-2024-50226 CVE-2024-50234 CVE-2024-50235 CVE-2024-50246 CVE-2024-50247 CVE-2024-50257 CVE-2024-50261 CVE-2024-50262 CVE-2024-50278 CVE-2024-50301 CVE-2024-53104 CVE-2024-53141 CVE-2024-53156 CVE-2024-53165 CVE-2024-53179 CVE-2024-56551 CVE-2024-56581 CVE-2024-56595 CVE-2024-56596 CVE-2024-56600 CVE-2024-56601 CVE-2024-56602 CVE-2024-56603 CVE-2024-56604 CVE-2024-56606 CVE-2024-56608 CVE-2024-56619 CVE-2024-56626 CVE-2024-56627 CVE-2024-56704 CVE-2024-56759 CVE-2024-56766 CVE-2024-56772 CVE-2024-57798 CVE-2024-57896 CVE-2024-57906 CVE-2024-57907 CVE-2024-57908 CVE-2024-57910 CVE-2024-57911 CVE-2024-57912 CVE-2024-57925 CVE-2024-57926 CVE-2024-57951 CVE-2024-58087 CVE-2024-8805 CVE-2025-21631 CVE-2025-21647 CVE-2025-21648 CVE-2025-21650 CVE-2025-21652 CVE-2025-21671 CVE-2025-21680 CVE-2025-21687 CVE-2025-21691 CVE-2025-21692 CVE-2025-21693 CVE-2025-21785 CVE-2025-21855 CVE-2025-21856 CVE-2025-21858 CVE-2025-21863 CVE-2025-21999 CVE-2025-23150

	CVE-2025-37738 CVE-2025-37750 CVE-2025-37785 CVE-2025-37797 CVE-2025-37800 CVE-2025-37813 CVE-2025-37831 CVE-2025-37863 CVE-2025-37878 CVE-2025-37892 CVE-2025-37937 CVE-2025-37938 CVE-2025-37943 CVE-2025-37944 CVE-2025-37979 CVE-2025-37982 CVE-2025-37988 CVE-2025-37989 CVE-2025-39735
krb5	CVE-2024-3596 CVE-2024-37370 CVE-2024-37371 CVE-2025-24528
ksh	CVE-2019-14868
kubernetes	CVE-2024-10220 CVE-2024-3177 CVE-2025-0426
lasso	CVE-2021-28091
leptonica	CVE-2020-36277 CVE-2020-36278 CVE-2020-36279 CVE-2020-36280 CVE-2020-36281 CVE-2022-38266
less	CVE-2022-46663 CVE-2024-32487
libEMF	CVE-2020-11863 CVE-2020-11864 CVE-2020-11865 CVE-2020-11866 CVE-2020-13999
libX11	CVE-2022-3554 CVE-2023-3138
libXpm	CVE-2022-44617 CVE-2022-46285 CVE-2022-4883
libarchive	CVE-2022-36227 CVE-2024-20696 CVE-2024-20697 CVE-2024-26256 CVE-2024-43495 CVE-2024-48957 CVE-2024-48958 CVE-2025-1632 CVE-2025-25724
libass	CVE-2020-26682 CVE-2020-36430
libcap	CVE-2025-1390
libconfuse	CVE-2022-40320
libcue	CVE-2023-43641
libdb	CVE-2019-2708
libdwarf	CVE-2024-2002

libesmtp	CVE-2019-19977
libfastjson	CVE-2020-12762
libgcrypt	CVE-2021-33560 CVE-2021-40528
libgit2	CVE-2020-12278 CVE-2020-12279 CVE-2024-24575 CVE-2024-24577
libgsf	CVE-2024-36474 CVE-2024-42415
libid3tag	CVE-2004-2779 CVE-2017-11550
libidn2	CVE-2019-12290
libksba	CVE-2022-3515 CVE-2022-47629
libldb	CVE-2022-32746 CVE-2023-0614
liblouis	CVE-2023-26769
libmicrohttpd	CVE-2023-27371
libmspack	CVE-2018-18585 CVE-2018-18586 CVE-2019-1010305
libndp	CVE-2024-5564
libosinfo	CVE-2019-13313
libpq	CVE-2021-32027 CVE-2022-1552 CVE-2023-5868 CVE-2024-4317
libproxy	CVE-2020-25219
librabbitmq	CVE-2019-18609 CVE-2023-35789
librepo	CVE-2020-14352
libreswan	CVE-2022-23094 CVE-2023-23009 CVE-2023-30570 CVE-2023-38710 CVE-2023-38711 CVE-2023-38712 CVE-2024-2357 CVE-2024-3652
libsass	CVE-2022-26592 CVE-2022-43357 CVE-2022-43358
libslirp	CVE-2021-3952

libsndfile	CVE-2021-3246 CVE-2021-4156 CVE-2024-50612 CVE-2203-33065
libsoup3	CVE-2024-52530 CVE-2024-52531 CVE-2024-52532
libssh	CVE-2023-1667 CVE-2023-2283 CVE-2023-48795 CVE-2023-6004 CVE-2023-6918
libssh2	CVE-2023-48795
libtar	CVE-2013-4420
libtasn1	CVE-2021-46848 CVE-2024-12133
libtiff	CVE-2023-25433 CVE-2023-26966 CVE-2023-2908 CVE-2023-3316 CVE-2023-3576 CVE-2023-6228 CVE-2023-6277 CVE-2024-7006
libtirpc	CVE-2021-46828
libtomcrypt	CVE-2019-17362
libtommath	CVE-2023-36328
libtpms	CVE-2021-3446 CVE-2021-3505 CVE-2021-3623 CVE-2021-3746 CVE-2023-1017
libupnp	CVE-2020-13848
libuv	CVE-2020-8252 CVE-2024-24806
libvirt	CVE-2024-4418
libvpx	CVE-2023-44488 CVE-2023-5217 CVE-2024-5197
libwebp	CVE-2023-1999 CVE-2023-4863
libxkbfile	CVE-2025-26595
libxml2	CVE-2023-45322 CVE-2024-25062 CVE-2024-34459 CVE-2024-40896 CVE-2024-56171 CVE-2025-24928 CVE-2025-27113 CVE-2025-32414 CVE-2025-32415
libxslt	CVE-2021-30560 CVE-2024-55549 CVE-2025-24855
libxsmm	CVE-2021-39535 CVE-2021-39536

libyaml	CVE-2024-3205
lighttpd	CVE-2022-22707 CVE-2022-37797 CVE-2022-41556
linux-firmware	CVE-2024-56161
linux-sgx	CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-2650 CVE-2023-3446 CVE-2023-3817 CVE-2023-5678 CVE-2024-5535
linuxptp	CVE-2021-3570 CVE-2021-3571
log4j	CVE-2020-9488
logback	CVE-2017-5929 CVE-2021-42550 CVE-2023-6378 CVE-2023-6481
logrotate	CVE-2022-1348
lua	CVE-2021-43519 CVE-2021-44647 CVE-2021-44964 CVE-2022-28805 CVE-2022-33099
luajit	CVE-2020-15890 CVE-2020-24372
lynx	CVE-2021-38165
lz4	CVE-2021-3520
m2crypto	CVE-2020-25657
mariadb	CVE-2022-27376 CVE-2022-27377 CVE-2022-27378 CVE-2022-27379 CVE-2022-27380 CVE-2022-27381 CVE-2022-27382 CVE-2022-27383 CVE-2022-27384 CVE-2022-27385 CVE-2022-27386 CVE-2022-27387 CVE-2022-27444 CVE-2022-27445 CVE-2022-27446 CVE-2022-27447 CVE-2022-27448 CVE-2022-27449 CVE-2022-27451 CVE-2022-27452 CVE-2022-27455 CVE-2022-27456 CVE-2022-27457 CVE-2022-27458 CVE-2024-21096
marked	CVE-2022-21680
maven	CVE-2021-26291
maven-shared-utils	CVE-2022-29599

mc	CVE-2021-36370
mcpp	CVE-2019-14274
memcached	CVE-2019-15026 CVE-2023-46852 CVE-2023-46853
microcode_ctl	CVE-2023-22655 CVE-2023-23583 CVE-2023-28746 CVE-2023-38575 CVE-2023-39368 CVE-2023-42667 CVE-2023-43490 CVE-2023-45733 CVE-2023-45745 CVE-2023-46103 CVE-2023-47855 CVE-2023-49141 CVE-2024-21820 CVE-2024-21853 CVE-2024-23918 CVE-2024-23984 CVE-2024-24853 CVE-2024-24968 CVE-2024-24980 CVE-2024-25939
moby	CVE-2024-29018 CVE-2024-41110
mod_auth_openidc	CVE-2019-20479 CVE-2021-20718 CVE-2021-39191 CVE-2023-28625 CVE-2024-24814
mod_fcgid	CVE-2016-1000104
mod_http2	CVE-2024-27316 CVE-2024-36387
mod_security	CVE-2021-42717
mod_security_crs	CVE-2019-11389 CVE-2022-39955 CVE-2022-39958
mojarra	CVE-2020-6950
mongo-c-driver	CVE-2023-0437 CVE-2024-6381 CVE-2024-6383
mosquitto	CVE-2021-34431 CVE-2021-34432 CVE-2021-41039 CVE-2023-28366 CVE-2023-3592
motif	CVE-2022-44617 CVE-2022-46285
mozjs102	CVE-2023-44488 CVE-2023-6209
mujs	CVE-2016-10141 CVE-2016-7504 CVE-2016-7506 CVE-2016-9017 CVE-2016-9108 CVE-2016-9136 CVE-2016-9294 CVE-2017-5627 CVE-2017-5628 CVE-2022-30974 CVE-2022-44789
musl	CVE-2020-28928

mutt	CVE-2020-14093 CVE-2020-14154 CVE-2020-28896 CVE-2021-3181 CVE-2022-1328 CVE-2023-4874 CVE-2023-4875
mx4j	CVE-2021-44228 CVE-2021-44832 CVE-2021-45105
mybatis	CVE-2020-26945 CVE-2021-44832
mysql-connector-java	CVE-2019-2692
nano	CVE-2024-5742
nasm	CVE-2019-20352 CVE-2020-24241 CVE-2022-44370
ncurses	CVE-2023-29491 CVE-2023-45918 CVE-2023-50495
nekohtml	CVE-2022-24839
net-snmp	CVE-2022-24805 CVE-2022-24806 CVE-2022-24807 CVE-2022-24808 CVE-2022-24809 CVE-2022-24810 CVE-2022-44792 CVE-2022-44793
nettle	CVE-2021-20305 CVE-2021-3580
netty	CVE-2021-37136 CVE-2021-37137 CVE-2021-43797 CVE-2021-45105 CVE-2022-41881 CVE-2024-29025
netty3	CVE-2019-16869 CVE-2019-20444 CVE-2019-20445 CVE-2024-29025
nghttp2	CVE-2023-35945 CVE-2023-44487 CVE-2024-28182
nginx	CVE-2023-44487 CVE-2024-7347 CVE-2025-23419
nodejs	CVE-2023-45853 CVE-2023-46809 CVE-2024-21892 CVE-2024-21896 CVE-2024-22018 CVE-2024-22019 CVE-2024-22020 CVE-2024-22025 CVE-2024-24758 CVE-2024-27982 CVE-2024-27983 CVE-2024-36137 CVE-2024-5274 CVE-2024-5535 CVE-2024-7971 CVE-2025-23083 CVE-2025-23084 CVE-2025-23085
nodejs-fstream	CVE-2019-13173

nodejs-getobject	CVE-2020-28282
nodejs-grunt	CVE-2020-7729 CVE-2022-0436
nodejs-handlebars	CVE-2021-23383
nodejs-hawk	CVE-2022-29167
nodejs-hosted-git-info	CVE-2021-23362
nodejs-jison	CVE-2020-8178
nodejs-minimist	CVE-2020-7598 CVE-2021-44906
nodejs-qs	CVE-2022-24999
nodejs-tough-cookie	CVE-2023-26136
nodejs-underscore	CVE-2021-23358
ntfs-3g	CVE-2022-40284 CVE-2023-52890
ntp	CVE-2023-26551 CVE-2023-26552 CVE-2023-26553 CVE-2023-26554 CVE-2023-26555
numpy	CVE-2021-34141 CVE-2021-41495 CVE-2021-41496
oniguruma	CVE-2019-19012
opencryptoki	CVE-2024-0914
openjpeg2	CVE-2021-3575 CVE-2022-1122 CVE-2023-39328 CVE-2024-56826 CVE-2024-56827
opensc	CVE-2021-34193 CVE-2023-2977 CVE-2023-40660 CVE-2023-40661 CVE-2023-4535 CVE-2023-5992 CVE-2024-45615 CVE-2024-45616 CVE-2024-45617 CVE-2024-45618 CVE-2024-45619 CVE-2024-45620 CVE-2024-8443
openslp	CVE-2019-5544
openssh	CVE-2024-39894 CVE-2025-26465 CVE-2025-26466 CVE-2025-32728
openssl	CVE-2024-13176

openvpn	CVE-2022-0547 CVE-2023-46849 CVE-2023-46850 CVE-2024-28882 CVE-2024-5594
openvswitch	CVE-2023-1668 CVE-2023-3966 CVE-2023-5366
optipng	CVE-2016-3981 CVE-2016-3982 CVE-2023-43907
opusfile	CVE-2022-47021
osc	CVE-2019-3681 CVE-2024-22034
p11-kit	CVE-2020-29361 CVE-2020-29362 CVE-2020-29363
pam	CVE-2024-10041 CVE-2024-10963 CVE-2024-22365
patchelf	CVE-2022-44940
pcp	CVE-2023-6917 CVE-2024-3019 CVE-2024-45769 CVE-2024-45770
pcre	CVE-2020-14155
pdfbox	CVE-2018-11797 CVE-2018-8036
perl	CVE-2023-47038 CVE-2023-47100 CVE-2023-48039 CVE-2024-56406
perl-CPAN	CVE-2023-31484
perl-DBI	CVE-2014-10402
perl-HTTP-Tiny	CVE-2023-31486
perl-Module-ScanDeps	CVE-2024-10224
pesign	CVE-2022-3560
pixman	CVE-2022-44638
pkgconf	CVE-2023-24056
pmix	CVE-2023-41915
podman	CVE-2022-3064 CVE-2023-3978 CVE-2023-48795 CVE-2024-1753 CVE-2024-28180

polkit	CVE-2021-4115
poppler	CVE-2022-27337 CVE-2022-38784 CVE-2024-56378 CVE-2024-6239 CVE-2025-32364 CVE-2025-32365 CVE-2025-43903
postgresql	CVE-2024-10976 CVE-2024-10977 CVE-2024-10978 CVE-2024-10979 CVE-2024-7348 CVE-2025-1094
postgresql-jdbc	CVE-2022-21724 CVE-2022-31197 CVE-2022-41946 CVE-2024-1597
ppp	CVE-2022-4603
proftpd	CVE-2023-48795 CVE-2023-51713 CVE-2024-48651
protobuf	CVE-2024-7254
protobuf-c	CVE-2022-33070
pyYAML	CVE-2020-14343
python-GitPython	CVE-2023-41040
python-PyMySQL	CVE-2024-36039
python-aiohttp	CVE-2023-37276 CVE-2023-47627 CVE-2023-49081 CVE-2023-49082 CVE-2024-23334 CVE-2024-23829 CVE-2024-27306 CVE-2024-30251 CVE-2024-42367 CVE-2024-52304
python-aiosmtpd	CVE-2024-27305 CVE-2024-34083
python-black	CVE-2024-21503
python-bottle	CVE-2020-28473 CVE-2022-31799
python-certifi	CVE-2022-23491 CVE-2023-37920 CVE-2023-40104
python-configobj	CVE-2023-26112
python-cryptography	CVE-2023-23931 CVE-2023-38325 CVE-2024-26130
python-dns	CVE-2023-29483

python-eventlet	CVE-2023-29483
python-flask-restx	CVE-2021-32838
python-gevent	CVE-2023-41419
python-httplib2	CVE-2020-11078 CVE-2021-21240
python-idna	CVE-2024-3651
python-jinja2	CVE-2024-22195 CVE-2024-34064 CVE-2024-56201 CVE-2024-56326 CVE-2025-27516
python-jupyter-server	CVE-2024-35178
python-jwcrypto	CVE-2023-6681 CVE-2024-28102
python-jwt	CVE-2022-29217
python-ldap	CVE-2021-46823
python-paramiko	CVE-2022-24302 CVE-2023-48795
python-pillow	CVE-2022-22815 CVE-2022-22816 CVE-2022-45199 CVE-2023-50447
python-pip	CVE-2023-45803 CVE-2024-37891
python-pycryptodome	CVE-2023-52323
python-pycryptodomex	CVE-2023-52323
python-pyinstaller	CVE-2023-49797
python-pymongo	CVE-2024-21506
python-reportlab	CVE-2019-17626 CVE-2023-33733
python-requests	CVE-2023-32681 CVE-2024-35195
python-rsa	CVE-2020-13757 CVE-2020-25658
python-rtslib	CVE-2020-14019

python-scikit-learn	CVE-2024-5206
python-setuptools	CVE-2022-40897 CVE-2024-6345
python-tornado	CVE-2023-28370 CVE-2024-52804 CVE-2025-47287
python-tqdm	CVE-2024-34062
python-twisted	CVE-2019-12855 CVE-2020-10108 CVE-2020-10109 CVE-2023-46137 CVE-2024-41671 CVE-2024-41810
python-ujson	CVE-2022-31116 CVE-2022-31117
python-urllib3	CVE-2023-43804 CVE-2023-45803 CVE-2024-37891
python-virtualenv	CVE-2024-53899
python-waitress	CVE-2022-24761 CVE-2024-49768 CVE-2024-49769
python-webob	CVE-2024-42353
python-werkzeug	CVE-2024-34069 CVE-2024-49767
python-zipp	CVE-2024-5569
python3	CVE-2023-27043 CVE-2023-6597 CVE-2024-0397 CVE-2024-0450 CVE-2024-3219 CVE-2024-4032 CVE-2024-6232 CVE-2024-6923 CVE-2024-7592 CVE-2024-8088 CVE-2024-9287 CVE-2025-0938
pytorch	CVE-2024-31584
qt	CVE-2023-32573 CVE-2023-34410 CVE-2023-37369 CVE-2023-38197 CVE-2023-43114
qt5-qtbase	CVE-2023-37369 CVE-2023-38197 CVE-2023-43114 CVE-2023-45935 CVE-2023-51714 CVE-2024-25580 CVE-2025-30348
qt5-qtsvg	CVE-2021-45930
qt5-qtwebengine	CVE-2023-6112

qt6-qtbase	CVE-2023-37369 CVE-2023-38197 CVE-2023-43114 CVE-2023-45935 CVE-2023-51714 CVE-2024-25580 CVE-2024-33861 CVE-2024-39936
qt6-qtwebengine	CVE-2023-6112
quartz	CVE-2019-13990
rapidjson	CVE-2024-38517
raptor2	CVE-2020-25713
rear	CVE-2024-23301
redis	CVE-2021-29478 CVE-2021-32626 CVE-2021-32627 CVE-2021-32628 CVE-2021-32672 CVE-2021-32675 CVE-2021-32687 CVE-2021-32762 CVE-2021-41099 CVE-2022-24735 CVE-2022-24736 CVE-2022-24834 CVE-2022-35977 CVE-2022-36021 CVE-2022-3647 CVE-2022-3734 CVE-2023-25155 CVE-2023-28856 CVE-2023-45145 CVE-2024-31228 CVE-2024-31449 CVE-2024-46981
resteasy	CVE-2016-9606 CVE-2020-10688 CVE-2021-20289
rpm-ostree	CVE-2024-2905
rsync	CVE-2020-14387 CVE-2022-29154 CVE-2022-37434 CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087 CVE-2024-12088 CVE-2024-12747
ruby	CVE-2024-27282 CVE-2024-35176 CVE-2024-35221 CVE-2024-39908 CVE-2024-41123 CVE-2024-41946 CVE-2024-43398 CVE-2024-47220 CVE-2024-49761 CVE-2025-25186 CVE-2025-27219 CVE-2025-27220 CVE-2025-27221
rubygem-actionmailer	CVE-2024-47889
rubygem-actionpack	CVE-2023-22797 CVE-2023-28362 CVE-2024-26143 CVE-2024-28103 CVE-2024-41128 CVE-2024-47887

rubygem-activerecord	CVE-2021-22880 CVE-2022-44566 CVE-2023-22794
rubygem-activeresource	CVE-2020-8151
rubygem-activestorage	CVE-2024-26144
rubygem-activesupport	CVE-2023-22796 CVE-2023-38037
rubygem-addressable	CVE-2021-32740
rubygem-bundler	CVE-2021-43809
rubygem-dalli	CVE-2022-4064
rubygem-excon	CVE-2019-16779
rubygem-globalid	CVE-2023-22799
rubygem-kramdown	CVE-2020-14001 CVE-2021-28834
rubygem-mini_magick	CVE-2019-13574
rubygem-nokogiri	CVE-2020-26247 CVE-2021-41098 CVE-2022-24836
rubygem-puma	CVE-2021-29509 CVE-2021-41136 CVE-2022-23634 CVE-2022-24790 CVE-2023-40175 CVE-2024-21647 CVE-2024-45614
rubygem-rack	CVE-2022-44570 CVE-2022-44571 CVE-2022-44572 CVE-2024-25126 CVE-2024-26141 CVE-2024-26146 CVE-2025-25184 CVE-2025-27111 CVE-2025-27610
rubygem-rails	CVE-2020-8162 CVE-2020-8165
rubygem-railties	CVE-2023-38037
rubygem-sinatra	CVE-2022-45442
rubygem-webrick	CVE-2024-47220

rubygem-websocket-extensions	CVE-2020-7663
rubygem-yard	CVE-2024-27285
runc	CVE-2024-45310
samba	CVE-2023-3961 CVE-2023-4091 CVE-2023-4154 CVE-2023-42669 CVE-2023-42670
sane-backends	CVE-2020-12861 CVE-2020-12862 CVE-2020-12863 CVE-2020-12864 CVE-2020-12865 CVE-2020-12866 CVE-2020-12867 CVE-2023-46047 CVE-2023-46052
sbt	CVE-2023-46122
screen	CVE-2021-26937 CVE-2023-24626
scsi-target-utils	CVE-2024-45751
shapelib	CVE-2022-0699
skopeo	CVE-2024-24786 CVE-2024-28180
snakeyaml	CVE-2022-25857 CVE-2022-38749 CVE-2022-38752 CVE-2022-41854
snappy-java	CVE-2023-34454 CVE-2023-34455 CVE-2023-43642
socat	CVE-2024-54661
spamassassin	CVE-2020-1930 CVE-2020-1931 CVE-2020-1946
speex	CVE-2020-23903
sphinx	CVE-2020-29050
spice	CVE-2020-14355 CVE-2021-20201
spice-vdagent	CVE-2020-25650 CVE-2020-25651 CVE-2020-25652 CVE-2020-25653
springframework	CVE-2016-5007 CVE-2020-5421
sqlite	CVE-2022-46908 CVE-2023-36191 CVE-2023-7104 CVE-2024-0232

squashfs-tools	CVE-2021-40153 CVE-2021-41072
squid	CVE-2023-46724 CVE-2023-46846 CVE-2023-46847 CVE-2023-46848 CVE-2023-49285 CVE-2023-49286 CVE-2023-50269 CVE-2023-5824 CVE-2024-25111 CVE-2024-37894 CVE-2024-45802
sssd	CVE-2023-3758
stb	CVE-2023-45662 CVE-2023-45663 CVE-2023-45664 CVE-2023-45666 CVE-2023-45667 CVE-2023-45675 CVE-2023-45681 CVE-2023-47212
strongswan	CVE-2022-40617 CVE-2023-41913
subversion	CVE-2024-45720 CVE-2024-46901
sudo	CVE-2023-22809 CVE-2023-27320 CVE-2023-28486 CVE-2023-28487
swtpm	CVE-2020-28407 CVE-2022-23645
syslinux	CVE-2011-2501 CVE-2011-2690 CVE-2011-2691 CVE-2011-2692 CVE-2011-3045 CVE-2011-3048 CVE-2012-3425 CVE-2015-7981 CVE-2015-8126 CVE-2015-8472 CVE-2015-8540 CVE-2016-10087 CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 CVE-2016-9843 CVE-2017-12652
sysstat	CVE-2023-33204
taglib	CVE-2018-11439
tang	CVE-2023-1672
tar	CVE-2021-20193 CVE-2022-48303
tcpdump	CVE-2023-1801 CVE-2024-2397
telnet	CVE-2020-10188 CVE-2022-39028
testng	CVE-2022-4065

texlive-base	CVE-2023-32700 CVE-2023-46048 CVE-2023-46051
thrift	CVE-2018-11798 CVE-2018-1320 CVE-2019-0205 CVE-2019-0210 CVE-2020-13949
tidy	CVE-2021-33391
tinyxml	CVE-2021-42260
tmux	CVE-2022-47016
tomcat	CVE-2021-43980 CVE-2022-25762 CVE-2022-42252 CVE-2023-24998 CVE-2023-28708 CVE-2023-28709 CVE-2023-41080 CVE-2023-42795 CVE-2023-44487 CVE-2023-45648 CVE-2023-46589 CVE-2024-21733 CVE-2024-23672 CVE-2024-24549 CVE-2024-34750 CVE-2024-50379 CVE-2024-52318 CVE-2024-54677 CVE-2025-24813
tpm2-tools	CVE-2024-29038
tpm2-tss	CVE-2023-22745 CVE-2024-29040
traceroute	CVE-2023-46316
transfig	CVE-2021-32280 CVE-2021-37529 CVE-2021-37530
trousers	CVE-2020-24330 CVE-2020-24331 CVE-2020-24332
tuned	CVE-2024-52336 CVE-2024-52337
uboot-tools	CVE-2022-30767 CVE-2022-33967 CVE-2022-34835
unbound	CVE-2023-50387 CVE-2023-50868 CVE-2024-1488 CVE-2024-33655 CVE-2024-43167 CVE-2024-43168 CVE-2024-8508
undertow	CVE-2019-3888 CVE-2020-10705 CVE-2020-10719 CVE-2021-3690 CVE-2023-1108 CVE-2023-1973 CVE-2023-5379 CVE-2024-4109
unixODBC	CVE-2024-1013
unzip	CVE-2019-13232 CVE-2021-4217 CVE-2022-0529 CVE-2022-0530

uriparser	CVE-2021-46141 CVE-2021-46142 CVE-2024-34402 CVE-2024-34403
usbredir	CVE-2021-3700
varnish	CVE-2021-36740 CVE-2022-23959 CVE-2022-38150 CVE-2022-45060 CVE-2023-44487 CVE-2024-30156
velocity	CVE-2020-13936
velocity-tools	CVE-2020-13959
vim	CVE-2024-43802 CVE-2024-47814 CVE-2025-1215 CVE-2025-22134 CVE-2025-24014 CVE-2025-26603 CVE-2025-29768
virglrenderer	CVE-2022-0135 CVE-2022-0175
vorbis-tools	CVE-2014-9640 CVE-2023-43361
vte	CVE-2012-2738
vte291	CVE-2024-37535
wavpack	CVE-2020-35738
webkit2gtk3	CVE-2023-28204 CVE-2023-32373 CVE-2023-32409 CVE-2023-39928 CVE-2024-40779 CVE-2024-40780 CVE-2024-4558
webkit2gtk4.1	CVE-2023-28204 CVE-2023-32373 CVE-2023-32409 CVE-2023-39928 CVE-2024-40779 CVE-2024-40780 CVE-2024-4558
webkit2gtk5.0	CVE-2023-28204 CVE-2023-32373 CVE-2023-32409 CVE-2023-39928 CVE-2024-40779 CVE-2024-40780 CVE-2024-4558
wget	CVE-2024-10524 CVE-2024-38428
wildfly-build-tools	CVE-2021-44832 CVE-2021-45105
wildfly-core	CVE-2021-44228 CVE-2021-45105

wildfly-security-manager	CVE-2021-45105
wireshark	CVE-2023-0666 CVE-2024-0208 CVE-2024-0209 CVE-2024-24476 CVE-2024-4853 CVE-2024-4854 CVE-2024-4855 CVE-2024-8250 CVE-2024-8645
woodstox-core	CVE-2022-40152
wpa_supplicant	CVE-2023-52160 CVE-2024-5290
xdg-utils	CVE-2020-27748
xerces-c	CVE-2018-1311
xerces-j2	CVE-2012-0881 CVE-2022-23437
xmlbeans	CVE-2021-23926
xmlgraphics-commons	CVE-2020-11988
xmlrpc	CVE-2019-17570
xmlrpc-c	CVE-2024-45490 CVE-2024-45491
xnio	CVE-2023-5685
xorg-x11-server-Xwayland	CVE-2023-6377 CVE-2023-6478 CVE-2023-6816 CVE-2024-0229 CVE-2024-0408 CVE-2024-0409 CVE-2024-31080 CVE-2024-31081 CVE-2024-31083
xstream	CVE-2021-43859 CVE-2022-40151 CVE-2022-41966 CVE-2024-47072
xterm	CVE-2021-27135 CVE-2022-24130
xz	CVE-2025-31115
yajl	CVE-2017-16516 CVE-2022-24795
yasm	CVE-2023-31975 CVE-2023-37732

zbar	CVE-2023-40889 CVE-2023-40890
zeromq	CVE-2021-20236
zlib	CVE-2018-25032 CVE-2022-37434 CVE-2023-45853
zsh	CVE-2019-20044 CVE-2021-45444
zstd	CVE-2022-4899
zvbi	CVE-2025-2173 CVE-2025-2174 CVE-2025-2175 CVE-2025-2176 CVE-2025-2177
zziplib	CVE-2018-16548 CVE-2018-17828 CVE-2020-18442 CVE-2024-39134