KYLINSOFT
麒麟软件

银河麒麟高级服务器操作系统V10 SP3交易增强版

版本发布说明

麒麟软件有限公司

2024年08月

1. 版本概述

此次发布的是针对核心交易低时延场景的操作系统定制化版本，版本名称是银河麒麟高级服务器操作系统 V10 SP3交易增强版。本文说明列举了版本发布的详细内容。

2. 版本信息

类型	版本信息
产品名称	中文：银河麒麟高级服务器操作系统 V10 SP3交易增强版 英文： Kylin Linux Advanced Server V10(Trading)
定制基线	基于银河麒麟高级服务器操作系统 V10 SP3 2403构建银河麒麟高级服务器操作系统 V10（Trading）系统镜像
ISO 名称	Kylin-Server-V10-SP3-2403-Release-Trading-20240813-ARM64.iso Kylin-Server-V10-SP3-2403-Release-Trading-20240813-x86_64.iso
发布格式	ISO 、虚拟机镜像 、容器镜像
版本查询	终端：输入cat /etc/.kyinfo

3. 技术参数

类型	参数信息
支持架构	ARM、X86
支持处理器型号	飞腾 ：FT-2000+/64 、腾云 S2500 、腾云 S5000C 鲲鹏 ：920 、920 V200 海光 ：海光 1 号、海光 2 号、海光 C86-3G、海光 C86-4G 兆芯 ：开胜 ZX-C+ 、开胜 KH-20000 、开胜 KH-30000 、开胜 K H-40000 系列 Intel/AMD 等服务器平台
支持固件类型	BIOS/UEFI
内核版本	4.19.90
Glibc 版本	2.28-98
GCC 版本	7.3.0-2020033101
Java 版本	java-11-openjdk-11.0.24.8 、java-1.8.0-openjdk-1.8.0.422
开发语言支持	C/C++ 、Java 、Go、Python 、Php 、Perl 、ruby 等

桌面环境	UKUI 2.0
中文支持	GB18030-2022
虚拟化	KVM/qemu/libvirt
授权方式	在线 、离线、KMS 机制
补丁更新	每周
客户群体	金融领域
配套文档	银河麒麟高级服务器操作系统 V10 SP3交易增强版安装手册 银河麒麟高级服务器操作系统 V10 SP3交易增强版系统管理员手册

4. 版本主要特性

- 新增x86架构下onload 的（kernel bypass网络协议栈）功能支持，版本onload 8.1.3.40，详细参照官网介绍。

- 该版本集成麒麟自研Gazelle功能模块，基于DPDK在用户态直接读写网卡报文，共享大页内存传递报文，使用轻量级LwIP协议栈，在满足高性能、高可用的同时，具备良好的通用性和易用性。

- 新增对MLNX_OFED_LINUX-驱动版本生态支持，现已支持版本包含：5.8-5.1.1.2-LTS（X86_64、aarch64）、23.10-3.2.2.0-LTS（X86_64、aarch64）。

5. 重要更新内容

5．1. 系统功能

5.1.1 系统组件

- anaconda： 安装程序设置交易环境为默认安装组；

- firefox： 火狐浏览器默认使用百度搜索引擎；

- glibc： 系统核心标准库功能增强和安全问题修复；
- grub2： Grub启动引导工具功能增强和安全问题修复；
- hardinfo： 系统信息工具修复未知传感器驱动和温度显示问题；
- httpd： 网页服务器功能增强和安全问题修复，禁用跟踪；
- openssl： 加密和SSL/TLS 工具安全问题修复；
- rpm： 包管理工具移除每日计划任务；
- shim： 安全启动组件添加 SMX 算法证书；
- systemd： 系统管理工具安全问题修复，修复更新设备符号链接问题，修复rc-local服务启动失败问题；
- udisks2： 磁盘管理工具修复udisksctl power-off命令执行问题；
- xorg-x11-server： 图形服务组件安全问题修复，修复飞腾S5000C平台花屏问题；

5.1.2 安全

- kysec-sync-daemon： 系统安全工具修复设备管控usb中的段错误；
- libboundscheck： 新增安全增强工具；
- mod_security： 安全模块安全问题修复；
- nss： 网络安全服务支持内核双签名；

5.1.3 容器和虚拟化

- docker-engine： 容器管理工具安全问题修复；
- libvirt： 虚拟化管理工具修复海光平台型号识别问题；

●qemu： Qemu虚拟化工具修复海光平台型号识别问题，支持海光CSV，修复迁移问题；

5.1.4 其他

- atril： 文档查看器安全问题修复；
- c-ares： 用于异步 DNS 请求的 C 语言库安全问题修复；
- copy-jdk-configs： JDK配置文件更新；
- curl： 下载工具安全问题修复；
- dpdk： 快速数据包处理的程序库和驱动程序集，问题修复与网络设备API适配；
- edk2： 固件开发工具修复 SEV 与 TPM 不兼容的问题；
- expat： XML 解析库安全问题修复；
- freerdp： 远程桌面连接工具安全问题修复；
- gazelle： 新增Gazelle高性能用户模式栈；
- glusterfs： Gluster文件系统问题修复，修复主机名验证问题；
- iotop： 进程监控更新，为 ioprio 添加 loongarch64 系统调用编号；
- java-1.8.0-openjdk： Java 8版本更新，进行安全问题修复，支持、兆芯、海光平台，修复cpu MP切换时原子操作稳定性问题；
- java-11-openjdk： Java 11版本更新，进行安全问题修复，支持、兆芯、海光平台；
- jose： JSON对象工具安全问题修复；
- kylin-control-center： 系统管理工具修复内存泄露问题；

- kylindoc： 系统文档更新desktop翻译；
- kylin-logos： 系统Logo组件更新KylinSoft版权信息；
- kylin-log-viewer： 系统日志查看工具安全问题修复；
- less： 文本文件分页查看工具安全问题修复；
- libarchive： 归档工具安全问题修复；
- libkylin-activation： 系统激活工具问题修复；
- libndp： 邻居发现协议库安全问题修复；
- libreswan： IPsec 协议库安全问题修复；
- libssh2： SSH 库安全问题修复；
- libtiff： 图像库安全问题修复；
- libxml2： XML 解析库安全问题修复；
- llvm： LLVM编译器安全问题修复；
- lwip： 新增LWIP网络协议栈组件；
- marco： 窗口管理器功能属性增强；
- mesa： Mesa图形库修复飞腾S5000C平台花屏问题；
- mod_http2： HTTP/2 模块安全问题修复；
- mozjs78： JavaScript 引擎安全问题修复；
- ncurses： 文本用户界面开发库安全问题修复；
- procps-ng： 系统信息提供工具修复gb18030下ps查看中文进程名显示乱码问题；

- python-idna： IDNA支持python库安全问题修复；
- python-setuptools： Python 包管理工具安全问题修复；
- qt： Qt开发库修复域对话框输入问题；
- rear： 备份恢复工具修复linuxefi创建问题；
- sqlite： Sqlite数据库安全问题修复；
- wget： 下载工具安全问题修复；
- yelp：帮助文档修复在 书签栏打开“所有帮助文档”出错问题；

5.2. 内核

系统内核小版本升级，由4.19.90-89.11-v2401 升级为4.19.90-89.15-v2401 ，新增了部分特性，对已识别缺陷进行了修复与处理，修复CVE 300多个，主要调整如下：

●功能新增

1.支持arm64平台潮汐调度

2.优化64k内核页下xfs写放大的问题

3.Arm64/X86 内核安全启动新增 SM 和 RSA 双重支持

4.新增飞腾 mailbox 驱动支持

5.新增飞腾 mailbox 驱动支持

6.海光 4 号 KVM 虚拟化增强支持

7.海光架构 HCT 算法引擎驱动更新至 2.0 版本

●问题修复

1.修复在底层虚拟化卡住时，virtio_gpu 未主动释放消耗的内存的问题

2.修复概率性出现 hugetlb 分配失败的问题

3.优化 Megaraid 的随机读性能偏低的问题

4.修复 scan_swap_map_slots 潜在的 Softlockup 问题

5.修复 bpf prog_array_map_poke_run 运行时崩溃问题

6.修复 KASAN: use-after-free in kthread_stop 的问题

7.修复 xfrm 在 decode_session6 函数时潜在的 Use-After-Free 问题

8.修复 net/rds 潜在的 Use-After-Free 崩溃问题

9.修复 vfat 在 guard_bio_eod 故障时，潜在的 IO hang 住的问题

10. 修复 hugetlb 在某些情况下 NUMA node 不连续而未正确执行遍历的问题

11. 修复 md 软 RAID 在 status_resync 时 softlockup 的问题

12. 修复 xfs 文件系统在 xfs/246 DEBUG 模式下，断言故障的问题

13. 修复 hisi_sas SATA 盘回 DMA Setup 帧长度异常时触发群体慢盘问题

14. 修复 hibmc 在 hibmc_unload 时潜在的空指针访问问题

15. 修复 ftracetest 在 destroy_hist_field 时潜在的 KASAN 越界访问问题

16. 修复 mmap 和 close 之间竞态而导致 KASAN qlist_free_all 内存故障的问题

17. 修复 tipc 在刷新任务时存在的竞态死锁问题

18. 修复海光 KVM 压测卡顿的问题

19. 修复 sysv_readpage 潜在的在不可睡眠区存在睡眠函数的问题

20. 修复 TXGBE/NGBE 第三方驱动潜在的网络故障而导致系统卡死的问题

21. 修复 XFS 文件系统在关闭未先唤醒相关线程的问题

22. 修复 usb_gadget_ep_match_desc 潜在的空指针访问问题

23. 修复 bpf_prog_put 潜在的空指针访问问题

24. 修复 UBSAN: undefined-behaviour in __block_write_full_page 的问题

25. 修复 mellanox 10G 卡，出现非法地址访问的问题
26. 修复 j1939 驱动潜在的 j1939_tp_txtimer Use-After-Free 崩溃问题
27. 修复 FT-S2500 自适应网络框架在虚拟机环境时潜在的内核崩溃问题
28. 修复 FT-S2500 在 KVM 压力的情况下，潜在的 CPU 无响应的问题
29. KYSEC修复设置安全扩展属性时存在的内存泄露问题
30. KYSEC调整 PCR hash 表大小，防止内存占用过大的问题
31. KYSEC修复安全 Hook 到 sb_kern_mount 潜在的内存泄露问题
32. KYSEC修复 KYSEC 在调用 ax99100_tcm_pcr_read 时内核崩溃的问题
33. KYSEC修复 kysec 在 dentry 潜在的内存泄露问题
34. KYSEC修复遍历挂载的文件节点而潜在的竞态卡住问题
35. KYSEC修复 kysec 访问 sb_sec 潜在的空指针崩溃问题
36. 修复vxlan模块register_netdevice失败时的处理逻辑

5.3. 仓库说明

版本仓库源与通用版本（SP3-2403）源地址保持一致（https://update.cs2c.com.cn/NS/V10/V10SP3-2403/），包含基础核心包（BaseOS）、升级软件包（Update）、扩展软件包（EPKL）

6. 重要的安全漏洞修复

- 内核安全漏洞修复（2个）

CVE-2024-36971 CVE-2024-1086

- 系统安全漏洞修复（108个）

CVE-2023-1916 CVE-2023-27043 CVE-2023-38633 CVE-2023-45733 CVE-2023-45745 CVE-2023-45918 CVE-2023-46049 CVE-2023-46103 CVE-2023-47855 CVE-2023-48795 CVE-2023-50229 CVE-2023-50387 CVE-2023-51698 CVE-2023-52076 CVE-2023-52323 CVE-2023-52425 CVE-2023-6816 CVE-2023-7104 CVE-2024-0229 CVE-2024-0408 CVE-2024-0409 CVE-2024-1048 CVE-2024-20696 CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20922 CVE-2024-20923 CVE-2024-20925 CVE-2024-20926 CVE-2024-20945 CVE-2024-20952 CVE-2024-21005 CVE-2024-21011 CVE-2024-21012 CVE-2024-21068 CVE-2024-21085 CVE-2024-21094 CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21144 CVE-2024-21145 CVE-2024-21147 CVE-2024-21885 CVE-2024-21886 CVE-2024-2398 CVE-2024-24789 CVE-2024-2511 CVE-2024-25629 CVE-2024-28085 CVE-2024-28757 CVE-2024-2961 CVE-2024-32462 CVE-2024-32487 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-34459 CVE-2024-36039 CVE-2024-3651 CVE-2024-41110 CVE-2024-4741 CVE-2024-5535 CVE-2024-5564 CVE-2024-6345 CVE-2024-6387 CVE-2019-17567 CVE-2021-29946 CVE-2021-45960 CVE-2022-22740 CVE-2022-2309 CVE-2022-25235 CVE-2022-34481 CVE-2022-48279 CVE-2022-48624 CVE-2023-23599 CVE-2023-23601 CVE-2023-23602 CVE-2023-29532 CVE-2023-3164 CVE-2023-38709 CVE-2023-50495 CVE-2023-50868 CVE-2023-50967 CVE-2023-52426 CVE-2024-2357 CVE-2024-24795 CVE-2024-25062 CVE-2024-27316 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-2024-38428

CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38476 CVE-2024-38477 CVE-2024-39573 CVE-2024-39884 KVE-2023-0902 KVE-2023-0903