



银河麒麟桌面操作系统
V10 SP1 2303 update2 更新发布说明

麒麟软件有限公司

2023 年 11 月

整体概述

银河麒麟桌面操作系统 V10 SP1 2303 update2 是银河麒麟桌面操作系统 V10 SP1 系列的小版本更新，与 V10 SP1 2107、V10 SP1 2203、V10 SP1 2303 版本已适配软硬件生态保持兼容，支持平滑升级，提供在线更新和离线更新两种方式。

新版本支持飞腾 FT-2000/4、飞腾腾锐 D2000、鲲鹏 920、龙芯 3A4000、龙芯 3A5000、海光 2 号、海光 3 号、兆芯开先 6000 系列、兆芯 KH-40000 系列、申威 831、海思麒麟 990、海思麒麟 9006C、海思麒麟 M900，支持 Intel 最新 12、13 代（6.1 内核定制版）酷睿处理器和最新的 AMD 处理器。新增对 GB18030-2022《信息技术 中文编码字符集》标准的支持，在桌面环境、系统设置、文件管理等易用性和交互体验一致性方面有极大提升，并修复了系统部分已知问题和 CVE 漏洞，给用户带来更加流畅、舒适、安全的使用体验。

新增特性及问题修复

新硬件支持

CPU 适配

- 新增支持兆芯 KH-40000 系列处理器
- 新增支持英特尔 13 代酷睿处理器（6.1 内核定制版仅供 HP 整机导入使用）

GPU 适配

- X86 架构新增支持象帝先天钧一号显卡

外设适配

- 新增支持敦泰、中天一维、品识指纹模块
- 新增支持上海移远 5G 模块

内核

- 新增 MGLRU 功能，内存回收优化，提升系统使用流畅度
- 支持飞腾 D2000 平台负温显示
- 海光平台支持 CSV、TPM、TDM、TPCM、CCP、HCT 驱动
- 支持申威平台虚拟化
- 显示虚拟化优化，提升虚拟机场景下系统的流畅度

系统安装

- 实现单硬盘、多硬盘自动分区配置文件统一与优化
- 修复安装系统时屏幕缩放默认为 150% 的问题
- 修复在龙芯 3A5000 平台上安装后无法正常进入桌面，系统黑屏卡死的问题
- 修复某些特定机型安装系统过了 grub 界面出现黑屏的问题
- 修复选择光盘启动项后无法进入直接安装和试用安装界面的问题
- 修复多硬盘自动安装系统，优先级较低的硬盘未被自动选择为数据盘的问题

系统激活

- 修复新适配的厂商库文件未集成，导致 ukey 激活失败的问题

桌面环境

- 新增窗口动效：多窗口分屏尺寸调整动效、对话框弹出动效、模态对话框提醒抖动动效、消息通知弹出动效、关闭消息弹窗动效、任务栏隐藏及显示动效
- 新增控件动效：滑动条动效、进度条动效、鼠标悬浮文字提示动效、级联菜单弹出动效、右键菜单弹出消失动效
- 新增模块动效：多任务视图新建工作区动效、删除工作区动效、删除应用窗口动效、拖拽排序工作区动效、移动应用到工作区动效、通知中心面板进出动效
- 新增支持 GB18030-2022 字体编码标准
- 新增支持使用输入法通过 GB18030-2022 内码输入生僻字等特殊汉字
- 修复修改时间格式，侧边栏偶现闪退的问题
- 修复系统长时间静置，系统卡死的问题

- 修复重启或关开机界面点击网络图标 Wi-Fi 按钮直接进入系统的问题
- 修复点击电源切换用户后系统黑屏的问题
- 修复点击开始菜单或侧边栏，在任务栏生成图标的问题
- 修复护眼模式和色温模式多次切换后，护眼模式不生效的问题
- 修复控制面板中任务栏相关内容未汉化的问题
- 修复应用固定到任务栏失败的问题
- 修复虚拟键盘无法唤出的问题
- 修复锁屏界面输入正确密码出现概率性不能登录系统的问题

系统设置

- 支持时间、日期长短格式设置
- 新增护眼模式和色温设置

任务栏

- 新增影音预览图多媒体控制，支持暂停、播放、上一首（曲）、下一首（曲）；
- 增加配置项，可设置任务栏窗口列表平铺或合并

快捷键

- 支持系统快捷键自定义
- 支持 win+方向键快捷键组合进行窗口控制
- 新增快捷键实现窗口一键投递和放大镜功能
- 完善了开始菜单、多任务视图、用户配置服务的快捷键
- 修复按放大镜快捷键 Win+"+"，系统屏幕缩放率无变化的问题

窗口管理器

- 支持根据显卡性能自动选择 xrender 或者 opengl 渲染，图形显示更流畅
- 新增远程显示器功能，支持对双设备进行扩展屏设置
- 修复操作影音时，窗口管理器异常，任务栏消失的问题
- 修复毛玻璃特效默认未启用的问题
- 修复点击多任务视图按钮会导致窗管崩溃的问题

文件管理器

- 新增支持长文件名，兼容文件名超过 255 字符文件
- 新增支持多文件批量重命名
- 新增文件管理器搜索进度条显示
- 新增支持文件管理器不同页签间文件拖拽复制
- 新增文件重命名修改文件后缀时需弹窗提醒，避免无效后缀导致无法打开
- 新增配置开关，支持以弹出新窗口的方式打开文件夹
- 支持数据盘或分区空间不足时拷贝文件进行弹窗预警
- 文件搜索速度优化，开启索引后提速 600%，未开启索引提速 10%
- 大文件和多文件拷贝速度优化，提速 30%
- 多文件显示优化，数量超过 1 万以上保持显示和排序流畅
- 修复在文件管理器中无法检索到文件夹中的文件的问题
- 修复从移动硬盘拷贝文件夹（包含大量文件）至本地，拷贝到 50%，文件管理器闪退的问题
- 修复发送桌面文件或家目录文件至 U 盘，文件管理器异常的问题
- 修复文件管理器提示“无法获取系统图标”，桌面图标缺失的问题

会话管理器

- 新增注销/关机/重启被阻塞时的弹窗提醒

分级冻结 1.0

- 通过引入分级冻结技术对应用进行分级管理，不同层级限制资源的申请量，提高应用运行流畅度，提高能耗利用率，提升系统续航时间

登录锁屏

- 新增可配置用户登录前特别提示页面
- 优化锁屏界面屏幕键盘 UI 样式
- 支持视频格式（MP4）屏保和图片格式的轮播（jpg 、 jpeg 、 bmp 、 dib 、 png 、 jfif 、 jpe 、 gif 、 tif 、 tiff 、 wdp 、 svg）

- 增加开启屏保最低时间“1 分钟”选项
- 新增登录过程动画，提升登录体验

笔记本触控板多指手势

- 增加双指滑动调节滑动条，调节音量与亮度的功能
- 支持三指触控手势呼出和收回全局搜索

网络

- 新增支持 DNS 高级配置
- 修复 X86 架构有线连接后网总是断连，并显示黄色叹号提示网络受限的问题
- 修复修改 DNS 与高级配置保存后无法再次打开高级配置界面的问题
- 修复重启后正常联网的系统，终端执行“sudo apt-get update”失败，之后网络不可用的问题
- 修复修改安全性后无法连接上 Wi-Fi 的问题
- 修复拔插外置无线网卡，移动热点界面信息不刷新的问题
- 修复连接隐藏 Wi-Fi 失败后，任务栏 Wi-Fi 列表仍然存在的问题
- 修复无线网卡不支持开启移动热点无相关提示的问题
- 修复属性界面 ipv6 地址信息无法保存的问题

蓝牙

- 新增支持蓝牙用户隔离，多用户场景下体验提升
- 新增蓝牙耳机控制音视频应用的播放、暂停等选项
- 支持蓝牙设备名称自定义
- 支持蓝牙音频的淡入特效，声音由低逐步上升到预设值
- 支持 aac 音频编码，提升音质
- 用户提示信息策略优化，提升交互体验
- 修复关闭飞行模式后，蓝牙未开启的问题
- 修复连接带 pin 码的蓝牙键盘失败的问题
- 修复多文件传输过程中，关闭传输窗口或者接收窗口仍继续传输的问题

- 修复安全中心关闭蓝牙接口或插拔蓝牙适配器，控制面板闪退的问题
- 修复当电脑不含蓝牙时，控制面板仍显示蓝牙界面的问题

电源管理

- 修复休眠唤醒后，休眠按钮消失的问题
- 修复存在 swap 分区时不存在休眠功能，一段时间后出现休眠功能的问题

系统应用

看图

- 修复桌面上的图片右键选择图片打印无打印弹窗的问题
- 修复无法通过开始菜单/任务栏快捷方式/桌面快捷方式打开看图的问题

截图

- 新增支持 OCR 功能，可识别截图区域中的文字
- 修复保存截图后首次使用 OCR 看图不能正确打开图片的问题
- 修复桌面/任务栏右键唤出菜单页面时，快捷键打开截图失败的问题

影音

- 新增支持播放 URL 路径视频
- 修复麒麟影音默认语言为英文的问题
- 修复点击打开文件夹按钮，软件闪退的问题
- 修复命令行调用方式播放链接视频失败的问题

录音

- 修复录音文件无法标记的问题

刻录

- 修复插入带有光盘的 USB 光驱，刻录软件局部会由中文变成英文的问题
- 修复 DVD-RW、CD-RW 光盘追加刻录同名文件夹，文件管理器闪退的问题

摄像头

- 修复外接摄像头延迟录像的问题
- 修复摄像头拍照/录像闪退的问题

便签贴

- 新增支持窗口自由缩放功能

系统监视器

- 新增托盘查看 cpu/内存/磁盘/网络占用率

归档管理器

- 支持 tar、tar.gz 等格式分卷压缩
- 修复打开分卷压缩文件，首次“复制到系统剪切板”成功，后续再次复制到剪切板报错的问题
- 修复解压 Windows 下创建的压缩文件后文件名称乱码的问题

工具箱

- 修复处理器最大主频显示 Unknown 的问题
- 修复将声卡全部禁用后点击启用一个声卡，所有声卡都会被启用的问题
- 修复右上角选项-帮助无法打开用户手册的问题
- 修复藏文环境下，硬件参数界面未全部藏文化的问题

麒麟扫描

- 支持自动安装完成适配的扫描仪驱动
- 修复 USB 连接无驱动扫描设备未被检测出来的问题
- 修复扫描文件另存为后闪退的问题
- 修复热插拔扫描仪，扫描闪退的问题

字体管理器

- 修复预览框粘贴超出 30 个字符，且存在空格时，最后一个字符乱码的问题

麒麟管家

- 用户反馈合并到麒麟管家“服务支持”，优化问题响应流程和响应速度
- 新增 windows 数据迁移工具，支持文件类型包括：office、图片、影音视频、压缩包、文件夹等
- 新增远程协助工具，可通过识别码和验证码快速远程，支持远程控制、文件传输、操作录制、操作日志、水印提示、体验评分、私有部署
- 修复不关闭百宝箱工具，仅关闭麒麟管家后重新打开失败的问题
- 修复远程协助运维端连接客户端失败的问题
- 修复 win 迁移工具删除文件后迁移失败的问题
- 修复 win 迁移工具迁移失败，文件完整性校验不通过的问题
- 修复问题反馈没有提交到工单系统的问题

多端协同

- 多端协调替代手机助手，用户体验升级
- 支持麒麟 PC 间发现设备、投屏、反控、文件共享、搜索文件
- 支持麒麟 PC 向 Android 大屏投屏
- 支持通过麒麟 PC 端键盘向 Android 端输入中文
- 支持在 Android 端上查看/下载麒麟 PC 端文件
- 修复麒麟设备端通过附近设备扫描无法扫描出安卓设备或麒麟 pc 设备的问题
- 修复多台麒麟设备同时连接 Wi-Fi 后，多端协同应用打开后卡死的问题
- 修复麒麟 PC 建立连接，在空间不足时传输文件，无提示且文件损坏的问题
- 修复麒麟 PC 之间或麒麟向安卓设备投屏失败，界面提示 error 的问题
- 修复建立多端协同连接后，文件右键菜单无“发送至多端协同”选项的问题

生物特征管理工具

- 修复安装品识指纹驱动后录入指纹，提示“打开设备失败”的问题
- 修复安装 X86 的品识指纹驱动后，插入品识设备无法连接驱动的问题

备份还原

- 修复任务栏和字体没有还原至备份点位置的问题
- 修复备份还原依赖包配置错误导致版本编译失败的问题
- 修复通过 grub 界面还原初始系统失败的问题

系统安全

- 新增支持国密、非国密算法证书的安全启动功能，防止系统关键组件被恶意篡改
- 新增基于应用 ID 的访问控制机制，优化执行控制、应用联网控制、文件保护、进程保护的流程，提升易用性
- 新增应用访问权限控制功能，管控应用对用户隐私数据的访问行为，保护数据安全
- 新增系统安全风险通知，提高用户对系统安全状态感知

安全中心

- 支持对账户密码进行国密算法加密，防止密码破解泄露
- 优化安全体检、账户保护、防火墙、外设管控，提升功能友好性
- 修复可信启动度量失败时，无法打开安全中心的问题
- 修复新安装的系统体检后发现远程服务和本地服务存在风险项的问题
- 修复病毒防护隔离区文件无法删除的问题
- 修复病毒扫描时界面显示英文的问题
- 修复安全中心缺少可信度量的问题
- 修复外设管控开关无法切换的问题
- 修复普通用户插入 U 盘，无授权弹窗的问题
- 修复应用访问权限控制，高级配置界面响应时间过长的的问题
- 修复应用访问权限控制应用列表未以应用名称展示，且分类全为其他软件的问题
- 修复关闭 wps 访问 home 目录下文件权限，仍可成功访问的问题
- 修复应用保护页面普通用户设置的权限同步到管理员账户的问题
- 修复应用防护控制防杀死保护按钮无法打开/关闭的问题

文件保护箱

- 修复普通用户打开文件保护箱，需要输入管理员用户密码授权的问题
- 修复文件保护箱搜索窗口输入任意值后软件闪退的问题

日志查看器

- 修复最新版本日志查看器首次打开点击“正常”，应用闪退的问题

三权分立

- 修复切换至 strict 模式后无法切换回 default 模式的问题

软件商店

- 优化客户端整体界面布局
- 新增卸载软件界面软件排序方式选择
- 新增客户端接入数量超过限制时弹窗提示
- 新增客户端软件详情页应用版本（kylin 版/windows 版/安卓版）区分
- 新增客户端搜索结果页按 kylin 版/windows 版/安卓版筛选
- 新增对某个软件忽略更新提示功能
- 新增支持删除历史安装记录
- 新增适配英文、藏文、繁体
- 新增“用户反馈”入口
- 新增支持外链广告
- 优化下载软件目录设置，支持选择系统目录
- 优化客户端搜索逻辑，提高应用搜索效率
- 修复软件商店安装 kwre 应用失败的问题
- 修复无法成功卸载软件，一直提示卸载中的问题
- 修复下载安装软件失败的问题

系统更新

- 新增支持系统升级错误码提示机制，在用户手册提供常见错误原因及修复建议

- 新增支持精准推送，可通过 IP、label、mac、sn、key 推送
- 新增支持跨版本分阶段升级
- 修复升级后重启系统黑屏或死机的问题
- 修复升级成功还原系统失败的问题
- 修复离线升级 SW 架构的麒麟系统，在备份后点击升级，升级工具闪退的问题
- 修复离线升级提示“检查更新失败（错误码：#0100）”的问题
- 修复在线更新无法及时更新源文件的问题
- 修复检测不到源管理器推送的更新的问题
- 修复在线升级时点击全部更新，控制面板闪退的问题
- 修复在线升级后，无“更新成功”弹窗的问题
- 修复升级后机器睡眠，按电源键唤醒，机器屏幕不亮的问题
- 修复系统升级时，报依赖冲突的问题
- 修复系统升级到 50%时提示更新失败的问题

Kylin SDK 2.2

- 新增 50 多个桌面应用、安全应用开发的系统信息获取与管控 API
- 新增统一系统的时间格式显示与存储单位显示 API，提升系统 UI 一致性
- 新增支持外设管控、软件包分级分类管控、软件包安装卸载黑白名单、关键进程状态监控等安全接口，加速了第三方安全套件适配
- 修复内置/外接摄像头信息无法获取的问题
- 修复获取短格式日期接口段错误的问题
- 修复笔记本显示器的最大分辨率和风扇接口报“已放弃（核心已转储）”的问题
- 修复软件包装卸黑白名单管控-卸载接口不可用的问题
- 修复 delApp 接口不生效的问题
- 修复网络策略新增接口报错的问题
- 修复软件防卸载接口不可用的问题

安全管控 3.9

- 增强数据动静态分析管理能力，并提升关键数据报表的准确性
- 完善总分一体的策略框架，实现多维度的策略管理
- 完成策略管理员分权的安全权限设计
- 完善多类型任务的可视化统一管理
- 增强高可用架构能力，支持双节点、三节点、多节点高可用能力
- 支持多级联合部署模式
- 多业务模块可视化能力提升
- 增强资产信息流转的安全及管理能力

云桌面

- 适配 8 家头部云桌面厂商：华为云、深信服云、锐捷云、阿里云、中兴云、海誉、升腾云、天翼云
- 完善云平台场景激活方案，支持授权回收

附录 修复的 CVE 安全漏洞清单

X86 架构安全漏洞修复列表

CVE-2022-32221、CVE-2022-43552、CVE-2022-4510、CVE-2023-29535、CVE-2023-29479、CVE-2023-29548、CVE-2023-29536、CVE-2023-1945、CVE-2023-29533、CVE-2023-29550、CVE-2023-29541、CVE-2023-0547、CVE-2023-29539 、 CVE-2022-38745 、 CVE-2023-27932 、 CVE-2023-25358 、 CVE-2023-28205 、 CVE-2022-32885、CVE-2022-0108、CVE-2023-27954、KVE-2022-0905、KVE-2021-1109、CVE-2023-2650、CVE-2023-1523、CVE-2023-32324、CVE-2023-2609、CVE-2023-2610、CVE-2021-45078、CVE-2023-32636、CVE-2023-32665 、 CVE-2023-24593 、 CVE-2023-32611 、 CVE-2023-29499 、 CVE-2023-25180 、 CVE-2023-32643、CVE-2022-2469、CVE-2023-3138、CVE-2022-4254、CVE-2022-45685、CVE-2022-45693、CVE-2022-40150、CVE-2022-40149、CVE-2022-24859、CVE-2023-2828、CVE-2020-27818、CVE-2020-35511、CVE-2023-34241、CVE-2023-1436、CVE-2021-28235、CVE-2023-3297、CVE-2023-3247、CVE-2023-33733、CVE-2023-1289、CVE-2021-20243、CVE-2021-20224、CVE-2021-20246、CVE-2021-20312、CVE-2021-20313、CVE-2021-20309 、 CVE-2021-39212 、 CVE-2021-20241 、 CVE-2022-32545 、 CVE-2022-28463 、 CVE-2021-20244 、 CVE-2023-34151 、 CVE-2020-29599 、 CVE-2022-32547 、 CVE-2022-32546 、 CVE-2023-34095 、 CVE-2023-36053 、 CVE-2023-25153 、 CVE-2023-25173 、 CVE-2023-34246 、 CVE-2023-36664 、 CVE-2023-36617 、 CVE-2023-28755 、 CVE-2023-29824 、 CVE-2023-25399 、 CVE-2022-40188、CVE-2022-37966、CVE-2022-45141、CVE-2022-37967、CVE-2022-42898、CVE-2022-3437、CVE-2022-38023、CVE-2021-20251、CVE-2023-0614、CVE-2023-0922、CVE-2022-4144、CVE-2022-1050、CVE-2023-0330、KVE-2023-0701、CVE-2023-34967、CVE-2023-34968、CVE-2023-34966、CVE-2022-2127、CVE-2023-28321 、 CVE-2023-28322 、 CVE-2021-26676 、 CVE-2022-32293 、 CVE-2023-28488 、 CVE-2022-23098 、 CVE-2021-26675 、 CVE-2021-33833 、 CVE-2022-23097 、 CVE-2022-23096 、 CVE-2022-32292、CVE-2020-21365、CVE-2022-24884、CVE-2023-20593、CVE-2022-4730、CVE-2022-4728、CVE-2022-4729、CVE-2022-21716、CVE-2022-21712、CVE-2019-9515、CVE-2019-9514、CVE-2019-9512、KVE-2023-0702、KVE-2023-0703、CVE-2020-13988、CVE-2020-13987、CVE-2020-17437、CVE-2023-20867、CVE-2023-22045 、 CVE-2023-22049 、 CVE-2023-22036 、 CVE-2023-25193 、 CVE-2023-22006 、 CVE-2023-22041 、 CVE-2023-38633 、 CVE-2023-37327 、 CVE-2023-37328 、 CVE-2023-31137 、 CVE-2022-30256、CVE-2022-2208、CVE-2022-2264、CVE-2022-2286、CVE-2022-2287、CVE-2022-2210、CVE-2022-2285、CVE-2022-2289、CVE-2022-2284、CVE-2022-2257、KVE-2023-0511、KVE-2022-0816、CVE-2021-25801 、 CVE-2021-25802 、 CVE-2022-41325 、 CVE-2021-25804 、 CVE-2021-25803 、 CVE-2020-13428 、 CVE-2020-13164 、 CVE-2020-17498 、 CVE-2020-15466 、 CVE-2020-25863 、 CVE-2020-25862、CVE-2023-22044、KVE-2023-0801、CVE-2022-2400、CVE-2021-3838、CVE-2020-13959、CVE-2020-13936、CVE-2022-3064、CVE-2021-4235、CVE-2022-40982、CVE-2023-23908、CVE-2022-41804、CVE-2022-48281、CVE-2023-2908、CVE-2023-3316、CVE-2023-3618、CVE-2023-38288、CVE-2023-25433、CVE-2023-38289 、 CVE-2023-26966 、 CVE-2023-26965 、 CVE-2020-36023 、 CVE-2020-36024 、 CVE-2023-40225、CVE-2020-18442、CVE-2018-7727、CVE-2023-38559、CVE-2023-39417、CVE-2023-20197、CVE-2022-39028、CVE-2023-40303、CVE-2023-37464、KVE-2023-0803、CVE-2021-32276、CVE-2021-32278、CVE-2023-38857 、 CVE-2021-32273 、 CVE-2021-32274 、 CVE-2021-32277 、 CVE-2023-38858 、 CVE-2021-32272 、 CVE-2021-33294 、 CVE-2020-21047 、 CVE-2023-20569 、 CVE-2023-40267 、 CVE-2023-22038 、 CVE-2023-22005 、 CVE-2023-22056 、 CVE-2023-22046 、 CVE-2023-22008 、 CVE-2023-22054 、 CVE-2023-22053 、 CVE-2023-22058 、 CVE-2023-22033 、 CVE-2023-22057 、 CVE-2023-22048、CVE-2022-3037、CVE-2022-3099、CVE-2022-3016、CVE-2022-2598、KVE-2023-0901、



CVE-2020-6097、CVE-2021-46671、CVE-2021-41054、CVE-2023-4049、CVE-2023-4056、CVE-2023-4047、CVE-2023-4045、CVE-2023-4050、CVE-2023-4046、CVE-2023-3417、CVE-2023-4048、CVE-2023-4055、CVE-2022-3520、CVE-2023-2253、CVE-2023-32627、KVE-2023-0902、KVE-2023-0903、CVE-2022-28737、CVE-2022-28734、CVE-2022-28735、CVE-2021-3697、CVE-2021-3981、CVE-2021-3696、CVE-2021-3695、CVE-2022-3775、CVE-2022-28736、CVE-2022-28733、CVE-2021-38714、CVE-2020-13933、CVE-2020-17510、CVE-2020-12460、CVE-2020-12272、KVE-2022-0406

ARM 架构安全漏洞修复列表

CVE-2022-32221、CVE-2022-43552、CVE-2022-4510、CVE-2023-29535、CVE-2023-29479、CVE-2023-29548、CVE-2023-29536、CVE-2023-1945、CVE-2023-29533、CVE-2023-29550、CVE-2023-29541、CVE-2023-0547、CVE-2023-29539、CVE-2022-38745、CVE-2023-27932、CVE-2023-25358、CVE-2023-28205、CVE-2022-32885、CVE-2022-0108、CVE-2023-27954、KVE-2022-0905、KVE-2021-1109、CVE-2023-2650、CVE-2023-1523、CVE-2023-32324、CVE-2023-2609、CVE-2023-2610、CVE-2021-45078、CVE-2023-32636、CVE-2023-32665、CVE-2023-24593、CVE-2023-32611、CVE-2023-29499、CVE-2023-25180、CVE-2023-32643、CVE-2022-2469、CVE-2023-3138、CVE-2022-4254、CVE-2022-45685、CVE-2022-45693、CVE-2022-40150、CVE-2022-40149、CVE-2022-24859、CVE-2023-2828、CVE-2020-27818、CVE-2020-35511、CVE-2023-34241、CVE-2023-1436、CVE-2021-28235、CVE-2023-3297、CVE-2023-3247、CVE-2023-33733、CVE-2023-1289、CVE-2021-20243、CVE-2021-20224、CVE-2021-20246、CVE-2021-20312、CVE-2021-20313、CVE-2021-20309、CVE-2021-39212、CVE-2021-20241、CVE-2022-32545、CVE-2022-28463、CVE-2021-20244、CVE-2023-34151、CVE-2020-29599、CVE-2022-32547、CVE-2022-32546、CVE-2023-34095、CVE-2023-36053、CVE-2023-25153、CVE-2023-25173、CVE-2023-34246、CVE-2023-36664、CVE-2023-36617、CVE-2023-28755、CVE-2023-29824、CVE-2023-25399、CVE-2022-40188、CVE-2022-37966、CVE-2022-45141、CVE-2022-37967、CVE-2022-42898、CVE-2022-3437、CVE-2022-38023、CVE-2021-20251、CVE-2023-0614、CVE-2023-0922、CVE-2022-4144、CVE-2022-1050、CVE-2023-0330、KVE-2023-0701、CVE-2023-34967、CVE-2023-34968、CVE-2023-34966、CVE-2022-2127、CVE-2023-28321、CVE-2023-28322、CVE-2021-26676、CVE-2022-32293、CVE-2023-28488、CVE-2022-23098、CVE-2021-26675、CVE-2021-33833、CVE-2022-23097、CVE-2022-23096、CVE-2022-32292、CVE-2020-21365、CVE-2022-24884、CVE-2023-20593、CVE-2022-4730、CVE-2022-4728、CVE-2022-4729、CVE-2022-21716、CVE-2022-21712、CVE-2019-9515、CVE-2019-9514、CVE-2019-9512、KVE-2023-0702、KVE-2023-0703、CVE-2020-13988、CVE-2020-13987、CVE-2020-17437、CVE-2023-20867、CVE-2023-22045、CVE-2023-22049、CVE-2023-22036、CVE-2023-25193、CVE-2023-22006、CVE-2023-22041、CVE-2023-38633、CVE-2023-37327、CVE-2023-37328、CVE-2023-31137、CVE-2022-30256、CVE-2022-2208、CVE-2022-2264、CVE-2022-2286、CVE-2022-2287、CVE-2022-2210、CVE-2022-2285、CVE-2022-2289、CVE-2022-2284、CVE-2022-2257、KVE-2023-0511、KVE-2022-0816、CVE-2021-25801、CVE-2021-25802、CVE-2022-41325、CVE-2021-25804、CVE-2021-25803、CVE-2020-13428、CVE-2020-13164、CVE-2020-17498、CVE-2020-15466、CVE-2020-25863、CVE-2020-25862、CVE-2023-22044、KVE-2023-0801、CVE-2022-2400、CVE-2021-3838、CVE-2020-13959、CVE-2020-13936、CVE-2022-3064、CVE-2021-4235、CVE-2022-40982、CVE-2023-23908、CVE-2022-41804、CVE-2022-48281、CVE-2023-2908、CVE-2023-3316、CVE-2023-3618、CVE-2023-38288、CVE-2023-25433、CVE-2023-38289、CVE-2023-26966、CVE-2023-26965、CVE-2020-36023、CVE-2020-36024、CVE-2023-40225、CVE-2020-18442、CVE-2018-7727、CVE-2023-38559、CVE-2023-39417、CVE-2023-20197、CVE-2022-39028、CVE-2023-40303、CVE-2023-37464、KVE-2023-0803、CVE-2021-32276、CVE-2021-32278、CVE-2023-38857、CVE-2021-32273、CVE-2021-32274、CVE-2021-32277、CVE-2023-38858、CVE-2021-32272、CVE-2021-33294、CVE-2020-21047、CVE-2023-20569、CVE-2023-40267、

CVE-2023-22038 、 CVE-2023-22005 、 CVE-2023-22056 、 CVE-2023-22046 、 CVE-2023-22008 、
CVE-2023-22054 、 CVE-2023-22053 、 CVE-2023-22058 、 CVE-2023-22033 、 CVE-2023-22057 、
CVE-2023-22048、CVE-2022-3037、CVE-2022-3099、CVE-2022-3016、CVE-2022-2598、KVE-2023-0901、
CVE-2020-6097、CVE-2021-46671、CVE-2021-41054、CVE-2023-4049、CVE-2023-4056、CVE-2023-4047、
CVE-2023-4045、CVE-2023-4050、CVE-2023-4046、CVE-2023-3417、CVE-2023-4048、CVE-2023-4055、
CVE-2022-3520、CVE-2023-2253、CVE-2023-32627、KVE-2023-0902、KVE-2023-0903、CVE-2022-28737、
CVE-2022-28734、CVE-2022-28735、CVE-2021-3697、CVE-2021-3981、CVE-2021-3696、CVE-2021-3695、
CVE-2022-3775、CVE-2022-28736、CVE-2022-28733、CVE-2021-38714、CVE-2020-13933、CVE-2020-17510、
CVE-2020-12460、CVE-2020-12272

MIPS 架构安全漏洞修复列表

CVE-2022-32221 、 CVE-2022-43552 、 CVE-2022-4510 、 CVE-2023-29535 、 CVE-2023-29479 、
CVE-2023-29548 、 CVE-2023-29536 、 CVE-2023-1945 、 CVE-2023-29533 、 CVE-2023-29550 、
CVE-2023-29541 、 CVE-2023-0547 、 CVE-2023-29539 、 CVE-2022-38745 、 CVE-2023-27932 、
CVE-2023-25358 、 CVE-2023-28205 、 CVE-2022-32885 、 CVE-2022-0108 、 CVE-2023-27954 、
KVE-2022-0905 、 KVE-2021-1109 、 CVE-2022-1304 、 CVE-2023-2650 、 CVE-2023-1523 、
CVE-2023-32324 、 CVE-2023-2609 、 CVE-2023-2610 、 CVE-2021-45078 、 CVE-2023-32636 、
CVE-2023-32665 、 CVE-2023-24593 、 CVE-2023-32611 、 CVE-2023-29499 、 CVE-2023-25180 、
CVE-2023-32643 、 CVE-2022-2469 、 CVE-2023-3138 、 CVE-2022-4254 、 CVE-2022-45685 、
CVE-2022-45693 、 CVE-2022-40150 、 CVE-2022-40149 、 CVE-2022-24859 、 CVE-2023-2828 、
CVE-2020-27818 、 CVE-2020-35511 、 CVE-2023-34241 、 CVE-2023-1436 、 CVE-2021-28235 、
CVE-2023-3297 、 CVE-2023-3247 、 CVE-2023-33733 、 CVE-2023-1289 、 CVE-2021-20243 、
CVE-2021-20224 、 CVE-2021-20246 、 CVE-2021-20312 、 CVE-2021-20313 、 CVE-2021-20309 、
CVE-2021-39212 、 CVE-2021-20241 、 CVE-2022-32545 、 CVE-2022-28463 、 CVE-2021-20244 、
CVE-2023-34151 、 CVE-2020-29599 、 CVE-2022-32547 、 CVE-2022-32546 、 CVE-2023-34095 、
CVE-2023-36053 、 CVE-2023-25153 、 CVE-2023-25173 、 CVE-2023-34246 、 CVE-2023-36664 、
CVE-2023-36617 、 CVE-2023-28755 、 CVE-2023-29824 、 CVE-2023-25399 、 CVE-2022-40188 、
CVE-2022-37966 、 CVE-2022-45141 、 CVE-2022-37967 、 CVE-2022-42898 、 CVE-2022-3437 、
CVE-2022-38023 、 CVE-2021-20251 、 CVE-2023-0614 、 CVE-2023-0922 、 CVE-2022-4144 、
CVE-2022-1050 、 CVE-2023-0330 、 KVE-2023-0701 、 CVE-2023-34967 、 CVE-2023-34968 、
CVE-2023-34966 、 CVE-2022-2127 、 CVE-2023-28321 、 CVE-2023-28322 、 CVE-2021-26676 、
CVE-2022-32293 、 CVE-2023-28488 、 CVE-2022-23098 、 CVE-2021-26675 、 CVE-2021-33833 、
CVE-2022-23097 、 CVE-2022-23096 、 CVE-2022-32292 、 CVE-2020-21365 、 CVE-2022-24884 、
CVE-2023-20593 、 CVE-2022-4730 、 CVE-2022-4728 、 CVE-2022-4729 、 CVE-2022-21716 、
CVE-2022-21712 、 CVE-2019-9515 、 CVE-2019-9514 、 CVE-2019-9512 、 KVE-2023-0702 、
KVE-2023-0703 、 CVE-2020-13988 、 CVE-2020-13987 、 CVE-2020-17437 、 CVE-2023-20867 、
CVE-2023-22045 、 CVE-2023-22049 、 CVE-2023-22036 、 CVE-2023-25193 、 CVE-2023-22006 、
CVE-2023-22041 、 CVE-2023-38633 、 CVE-2023-37327 、 CVE-2023-37328 、 CVE-2023-31137 、
CVE-2022-30256 、 CVE-2022-2208 、 CVE-2022-2264 、 CVE-2022-2286 、 CVE-2022-2287 、
CVE-2022-2210、CVE-2022-2285、CVE-2022-2289、CVE-2022-2284、CVE-2022-2257、KVE-2023-0511、
KVE-2022-0816 、 CVE-2021-25801 、 CVE-2021-25802 、 CVE-2022-41325 、 CVE-2021-25804 、
CVE-2021-25803 、 CVE-2020-13428 、 CVE-2020-13164 、 CVE-2020-17498 、 CVE-2020-15466 、
CVE-2020-25863 、 CVE-2020-25862 、 CVE-2023-22044 、 KVE-2023-0801 、 CVE-2022-2400 、
CVE-2021-3838 、 CVE-2020-13959 、 CVE-2020-13936 、 CVE-2022-3064 、 CVE-2021-4235 、

CVE-2022-40982 、 CVE-2023-23908 、 CVE-2022-41804 、 CVE-2022-48281 、 CVE-2023-2908 、
CVE-2023-3316 、 CVE-2023-3618 、 CVE-2023-38288 、 CVE-2023-25433 、 CVE-2023-38289 、
CVE-2023-26966 、 CVE-2023-26965 、 CVE-2020-36023 、 CVE-2020-36024 、 CVE-2023-40225 、
CVE-2020-18442 、 CVE-2018-7727 、 CVE-2023-38559 、 CVE-2023-39417 、 CVE-2023-20197 、
CVE-2022-39028 、 CVE-2023-40303 、 CVE-2023-37464 、 CVE-2021-32276 、 CVE-2021-32278 、
CVE-2023-38857 、 CVE-2021-32273 、 CVE-2021-32274 、 CVE-2021-32277 、 CVE-2023-38858 、
CVE-2021-32272 、 CVE-2021-33294 、 CVE-2020-21047 、 CVE-2023-20569 、 CVE-2023-40267 、
CVE-2023-22038 、 CVE-2023-22005 、 CVE-2023-22056 、 CVE-2023-22046 、 CVE-2023-22008 、
CVE-2023-22054 、 CVE-2023-22053 、 CVE-2023-22058 、 CVE-2023-22033 、 CVE-2023-22057 、
CVE-2023-22048 、 CVE-2022-3037 、 CVE-2022-3099 、 CVE-2022-3016 、 CVE-2022-2598 、
CVE-2023-0901 、 CVE-2020-6097 、 CVE-2021-46671 、 CVE-2021-41054 、 CVE-2023-4049 、
CVE-2023-4056 、 CVE-2023-4047 、 CVE-2023-4045 、 CVE-2023-4050 、 CVE-2023-4046 、 CVE-2023-3417 、
CVE-2023-4048 、 CVE-2023-4055 、 CVE-2022-3520 、 CVE-2023-2253 、 CVE-2023-32627 、
CVE-2023-0902 、 CVE-2023-0903 、 CVE-2022-28737 、 CVE-2022-28734 、 CVE-2022-28735 、
CVE-2021-3697 、 CVE-2021-3981 、 CVE-2021-3696 、 CVE-2021-3695 、 CVE-2022-3775 、
CVE-2022-28736 、 CVE-2022-28733 、 CVE-2021-38714 、 CVE-2020-13933 、 CVE-2020-17510 、
CVE-2020-12460 、 CVE-2020-12272

LoongArch 架构安全漏洞修复列表

CVE-2022-32221 、 CVE-2022-43552 、 CVE-2022-4510 、 CVE-2023-29535 、 CVE-2023-29479 、 CVE-2023-29548 、
CVE-2023-29536 、 CVE-2023-1945 、 CVE-2023-29533 、 CVE-2023-29550 、 CVE-2023-29541 、 CVE-2023-0547 、
CVE-2023-29539 、 CVE-2022-38745 、 CVE-2023-27932 、 CVE-2023-25358 、 CVE-2023-28205 、
CVE-2022-32885 、 CVE-2022-0108 、 CVE-2023-27954 、 CVE-2022-0905 、 CVE-2021-1109 、 CVE-2023-2650 、
CVE-2023-1523 、 CVE-2023-32324 、 CVE-2023-2609 、 CVE-2023-2610 、 CVE-2023-32636 、 CVE-2023-32665 、
CVE-2023-24593 、 CVE-2023-32611 、 CVE-2023-29499 、 CVE-2023-25180 、 CVE-2023-32643 、 CVE-2022-2469 、
CVE-2023-3138 、 CVE-2022-4254 、 CVE-2022-45685 、 CVE-2022-45693 、 CVE-2022-40150 、 CVE-2022-40149 、
CVE-2022-24859 、 CVE-2023-2828 、 CVE-2020-27818 、 CVE-2020-35511 、 CVE-2023-34241 、 CVE-2023-1436 、
CVE-2021-28235 、 CVE-2023-3297 、 CVE-2023-3247 、 CVE-2023-33733 、 CVE-2023-1289 、 CVE-2021-20243 、
CVE-2021-20224 、 CVE-2021-20246 、 CVE-2021-20312 、 CVE-2021-20313 、 CVE-2021-20309 、
CVE-2021-39212 、 CVE-2021-20241 、 CVE-2022-32545 、 CVE-2022-28463 、 CVE-2021-20244 、
CVE-2023-34151 、 CVE-2020-29599 、 CVE-2022-32547 、 CVE-2022-32546 、 CVE-2023-34095 、
CVE-2023-36053 、 CVE-2023-25153 、 CVE-2023-25173 、 CVE-2023-34246 、 CVE-2023-36664 、
CVE-2023-36617 、 CVE-2023-28755 、 CVE-2023-29824 、 CVE-2023-25399 、 CVE-2022-40188 、
CVE-2022-37966 、 CVE-2022-45141 、 CVE-2022-37967 、 CVE-2022-42898 、 CVE-2022-3437 、 CVE-2022-38023 、
CVE-2021-20251 、 CVE-2023-0614 、 CVE-2023-0922 、 CVE-2022-4144 、 CVE-2022-1050 、 CVE-2023-0330 、
CVE-2023-0701 、 CVE-2023-34967 、 CVE-2023-34968 、 CVE-2023-34966 、 CVE-2022-2127 、 CVE-2023-28321 、
CVE-2023-28322 、 CVE-2021-26676 、 CVE-2022-32293 、 CVE-2023-28488 、 CVE-2022-23098 、
CVE-2021-26675 、 CVE-2021-33833 、 CVE-2022-23097 、 CVE-2022-23096 、 CVE-2022-32292 、
CVE-2020-21365 、 CVE-2022-24884 、 CVE-2023-20593 、 CVE-2022-4730 、 CVE-2022-4728 、 CVE-2022-4729 、
CVE-2022-21716 、 CVE-2022-21712 、 CVE-2019-9515 、 CVE-2019-9514 、 CVE-2019-9512 、 CVE-2023-0702 、
CVE-2023-0703 、 CVE-2020-13988 、 CVE-2020-13987 、 CVE-2020-17437 、 CVE-2023-20867 、 CVE-2023-22045 、
CVE-2023-22049 、 CVE-2023-22036 、 CVE-2023-25193 、 CVE-2023-22006 、 CVE-2023-22041 、
CVE-2023-38633 、 CVE-2023-37327 、 CVE-2023-37328 、 CVE-2023-31137 、 CVE-2022-30256 、 CVE-2022-2208 、
CVE-2022-2264 、 CVE-2022-2286 、 CVE-2022-2287 、 CVE-2022-2210 、 CVE-2022-2285 、 CVE-2022-2289 、

CVE-2022-2284、CVE-2022-2257、KVE-2023-0511、KVE-2022-0816、CVE-2021-25801、CVE-2021-25802、CVE-2022-41325 、 CVE-2021-25804 、 CVE-2021-25803 、 CVE-2020-13428 、 CVE-2020-13164 、 CVE-2020-17498、CVE-2020-15466、CVE-2020-25863、CVE-2020-25862、CVE-2023-22044、CVE-2022-2400、CVE-2021-3838、CVE-2020-13959、CVE-2020-13936、CVE-2022-3064、CVE-2021-4235、CVE-2022-40982、CVE-2023-23908、CVE-2022-41804、CVE-2022-48281、CVE-2023-2908、CVE-2023-3316、CVE-2023-3618、CVE-2023-38288 、 CVE-2023-25433 、 CVE-2023-38289 、 CVE-2023-26966 、 CVE-2023-26965 、 CVE-2020-36023、CVE-2020-36024、CVE-2023-40225、CVE-2020-18442、CVE-2018-7727、CVE-2023-38559、CVE-2023-39417 、 CVE-2023-20197 、 CVE-2022-39028 、 CVE-2023-40303 、 CVE-2023-37464 、 CVE-2021-32276 、 CVE-2021-32278 、 CVE-2023-38857 、 CVE-2021-32273 、 CVE-2021-32274 、 CVE-2021-32277 、 CVE-2023-38858 、 CVE-2021-32272 、 CVE-2021-33294 、 CVE-2020-21047 、 CVE-2023-20569 、 CVE-2023-40267 、 CVE-2023-22038 、 CVE-2023-22005 、 CVE-2023-22056 、 CVE-2023-22046 、 CVE-2023-22008 、 CVE-2023-22054 、 CVE-2023-22053 、 CVE-2023-22058 、 CVE-2023-22033、CVE-2023-22057、CVE-2023-22048、CVE-2022-3037、CVE-2022-3099、CVE-2022-3016、CVE-2022-2598、KVE-2023-0901、CVE-2020-6097、CVE-2021-46671、CVE-2021-41054、CVE-2023-4049、CVE-2023-4056、CVE-2023-4047、CVE-2023-4045、CVE-2023-4050、CVE-2023-4046、CVE-2023-3417、CVE-2023-4048、CVE-2023-4055、CVE-2022-3520、CVE-2023-2253、CVE-2023-32627、KVE-2023-0902、KVE-2023-0903、CVE-2022-28737、CVE-2022-28734、CVE-2022-28735、CVE-2021-3697、CVE-2021-3981、CVE-2021-3696、CVE-2021-3695、CVE-2022-3775、CVE-2022-28736、CVE-2022-28733、CVE-2021-38714、CVE-2020-13933、CVE-2020-17510、CVE-2020-12460、CVE-2020-12272

SW 架构安全漏洞修复列表

CVE-2022-32221、CVE-2022-43552、CVE-2022-4510、CVE-2023-29535、CVE-2023-29479、CVE-2023-29548、CVE-2023-29536、CVE-2023-1945、CVE-2023-29533、CVE-2023-29550、CVE-2023-29541、CVE-2023-0547、CVE-2023-29539 、 CVE-2022-38745 、 CVE-2023-27932 、 CVE-2023-25358 、 CVE-2023-28205 、 CVE-2022-32885、CVE-2022-0108、CVE-2023-27954、KVE-2022-0905、KVE-2021-1109、CVE-2023-2650、CVE-2023-1523、CVE-2023-32324、CVE-2023-2609、CVE-2023-2610、CVE-2023-32636、CVE-2023-32665、CVE-2023-24593、CVE-2023-32611、CVE-2023-29499、CVE-2023-25180、CVE-2023-32643、CVE-2022-2469、CVE-2023-3138、CVE-2022-4254、CVE-2022-45685、CVE-2022-45693、CVE-2022-40150、CVE-2022-40149、CVE-2022-24859、CVE-2023-2828、CVE-2020-27818、CVE-2020-35511、CVE-2023-34241、CVE-2023-1436、CVE-2021-28235、CVE-2023-3297、CVE-2023-3247、CVE-2023-33733、CVE-2023-1289、CVE-2021-20243、CVE-2021-20224 、 CVE-2021-20246 、 CVE-2021-20312 、 CVE-2021-20313 、 CVE-2021-20309 、 CVE-2021-39212 、 CVE-2021-20241 、 CVE-2022-32545 、 CVE-2022-28463 、 CVE-2021-20244 、 CVE-2023-34151 、 CVE-2020-29599 、 CVE-2022-32547 、 CVE-2022-32546 、 CVE-2023-34095 、 CVE-2023-36053 、 CVE-2023-25153 、 CVE-2023-25173 、 CVE-2023-34246 、 CVE-2023-36664 、 CVE-2023-36617 、 CVE-2023-28755 、 CVE-2023-29824 、 CVE-2023-25399 、 CVE-2022-40188 、 CVE-2022-37966、CVE-2022-45141、CVE-2022-37967、CVE-2022-42898、CVE-2022-3437、CVE-2022-38023、CVE-2021-20251、CVE-2023-0614、CVE-2023-0922、CVE-2022-4144、CVE-2022-1050、CVE-2023-0330、KVE-2023-0701、CVE-2023-34967、CVE-2023-34968、CVE-2023-34966、CVE-2022-2127、CVE-2023-28321、CVE-2023-28322 、 CVE-2021-26676 、 CVE-2022-32293 、 CVE-2023-28488 、 CVE-2022-23098 、 CVE-2021-26675 、 CVE-2021-33833 、 CVE-2022-23097 、 CVE-2022-23096 、 CVE-2022-32292 、 CVE-2020-21365、CVE-2022-24884、CVE-2023-20593、CVE-2022-4730、CVE-2022-4728、CVE-2022-4729、CVE-2022-21716、CVE-2022-21712、CVE-2019-9515、CVE-2019-9514、CVE-2019-9512、KVE-2023-0702、KVE-2023-0703、CVE-2020-13988、CVE-2020-13987、CVE-2020-17437、CVE-2023-20867、CVE-2023-22045、CVE-2023-22049 、 CVE-2023-22036 、 CVE-2023-25193 、 CVE-2023-22006 、 CVE-2023-22041 、

CVE-2023-38633、CVE-2023-37327、CVE-2023-37328、CVE-2023-31137、CVE-2022-30256、CVE-2022-2208、CVE-2022-2264、CVE-2022-2286、CVE-2022-2287、CVE-2022-2210、CVE-2022-2285、CVE-2022-2289、CVE-2022-2284、CVE-2022-2257、KVE-2023-0511、KVE-2022-0816、CVE-2021-25801、CVE-2021-25802、CVE-2022-41325 、 CVE-2021-25804 、 CVE-2021-25803 、 CVE-2020-13428 、 CVE-2020-13164 、 CVE-2020-17498、CVE-2020-15466、CVE-2020-25863、CVE-2020-25862、CVE-2023-22044、CVE-2022-2400、CVE-2021-3838、CVE-2020-13959、CVE-2020-13936、CVE-2022-3064、CVE-2021-4235、CVE-2022-40982、CVE-2023-23908、CVE-2022-41804、CVE-2022-48281、CVE-2023-2908、CVE-2023-3316、CVE-2023-3618、CVE-2023-38288 、 CVE-2023-25433 、 CVE-2023-38289 、 CVE-2023-26966 、 CVE-2023-26965 、 CVE-2020-36023、CVE-2020-36024、CVE-2023-40225、CVE-2020-18442、CVE-2018-7727、CVE-2023-38559、CVE-2023-39417 、 CVE-2023-20197 、 CVE-2022-39028 、 CVE-2023-40303 、 CVE-2023-37464 、 CVE-2021-32276 、 CVE-2021-32278 、 CVE-2023-38857 、 CVE-2021-32273 、 CVE-2021-32274 、 CVE-2021-32277 、 CVE-2023-38858 、 CVE-2021-32272 、 CVE-2021-33294 、 CVE-2020-21047 、 CVE-2023-20569 、 CVE-2023-40267 、 CVE-2023-22038 、 CVE-2023-22005 、 CVE-2023-22056 、 CVE-2023-22046 、 CVE-2023-22008 、 CVE-2023-22054 、 CVE-2023-22053 、 CVE-2023-22058 、 CVE-2023-22033、CVE-2023-22057、CVE-2023-22048、CVE-2022-3037、CVE-2022-3099、CVE-2022-3016、CVE-2022-2598、KVE-2023-0901、CVE-2020-6097、CVE-2021-46671、CVE-2021-41054、CVE-2023-4049、CVE-2023-4056、CVE-2023-4047、CVE-2023-4045、CVE-2023-4050、CVE-2023-4046、CVE-2023-3417、CVE-2023-4048、CVE-2023-4055、CVE-2022-3520、CVE-2023-2253、CVE-2023-32627、KVE-2023-0902、KVE-2023-0903、CVE-2022-28737、CVE-2022-28734、CVE-2022-28735、CVE-2021-3697、CVE-2021-3981、CVE-2021-3696、CVE-2021-3695、CVE-2022-3775、CVE-2022-28736、CVE-2022-28733、CVE-2021-38714、CVE-2020-13933、CVE-2020-17510、CVE-2020-12460、CVE-2020-12272