KYLINSOFT
麒麟软件

银河麒麟桌面操作系统 V10 SP1 2503
版本发布说明

麒麟软件有限公司

2025 年 4 月

整体概述

银河麒麟桌面操作系统 V10 SP1 2503 是银河麒麟桌面操作系统 V10 SP1 系列的小版本更新，应用生态完全兼容，支持平滑升级。支持飞腾 FT-2000/4、飞腾 D2000、飞腾 D3000、鲲鹏 920、龙芯 3A4000、龙芯 3A5000、龙芯 3A6000 系列、海光 2 号、海光 C86-3G、海光 C86-4G、兆芯开先系列 (KX-7000 系列、KX-6000G、KX-6000、KX-5000、ZX-C+、ZX-C) 、兆芯开胜 KH-40000 系列、申威 SW-WY831、Kirin 990、Kirin 9006C、Kirin 9000C、pangu M900，支持 Intel 和 AMD 的主流处理器；内核和核心组件与前序版本保持一致；桌面环境、系统功能、安全、应用等易用性获得极大体验提升。

对比银河麒麟桌面操作系统 V10 SP1 2403，银河麒麟桌面操作系统 V10 SP1 2503 变更模块主要包括：

- **新增功能及优化**：新硬件支持，桌面环境（文件管理器、设置、显示器、任务栏、鼠标、登录与锁屏），软件商店，系统应用（麒麟管家、看图、音乐、截图、归档管理器、备份还原），AI 应用（AI 助手、记忆地图、数据管家、智能模糊搜索、麒麟速记），系统安全、系统激活，系统更新，Kylin SDK 2.5，AI 子系统
- **系统问题修复**：桌面环境（文件管理器、任务栏、窗口管理器、侧边栏、显示、声音、网络、截屏），系统应用（影音、音乐、看图、麒麟管家、打印机、扫描、刻录归档管理器、截图），系统安全（安全中心、文件保护箱），桌面环境、系统更新等
- **已经集成的漏洞补丁：见附录**
- **核心组件版本：**

表 1 核心组件清单

组件	V10 SP1 2403	V10 SP1 2503
Kernel	5.4、5.10/5.15（Intel、AMD）	5.4、5.10/5.15（Intel、AMD）
glibc	2.31、2.28（龙芯 3A5000、龙芯 3A6000）	2.31、2.28 (龙芯 3A5000、龙芯 3A6000)
gcc	9.3.0、8.3.0（龙芯 3A5000、	9.3.0、8.3.0（龙芯 3A5000、

	龙芯 3A6000）	龙芯 3A6000）
qt	5.12.12、4.8.7	5.12.12、4.8.7
gtk	2.24、3.24	2.24、3.24
systemd	245	245

新增和优化功能和特性

新硬件支持

CPU

- 新增支持兆芯开先 KX-6900 系列（KX-U6980S、KX-6940S）处理器
- 新增支持龙芯 3A6000-E

GPU

- 新增支持凌久微 GP202 显卡
- 新增支持芯瞳 CQ2040 显卡
- 新增支持摩尔 X300/X100 显卡
- 新增支持格兰菲 Arise 2030 显卡
- 新增格兰菲 Arise-GT-10C0t 芯片

网卡

- 新增支持景略半导体 jl2201 PHY 芯片
- 新增支持深蕾 SN6186 声卡支持
- 新增支持光润通 FF1002E-V3.0/FF902E-V3.0/FF902T-V3.0 网卡；
- 新增 Realtek USB WiFi&蓝牙支持
- 更新速通 SCM2625 模块驱动
- 更新裕太 YT6801 网卡驱动更新
- 更新瑞昱 PCIe 无线网卡&蓝牙驱动

内核

- 新增支持国民技术 Z32H330TC-SQN-755 SPI 接口的 TPM2.0
- 新增海光 C86-4G 虚拟化功能支持、安全设备支持，新增密钥管理系统 TKM 和国内可信计算规范 TCM2.0；以及海光平台内核性能优化
- 新增兆芯 CPU 硬件虚拟化技术。同时支持 SM2/SM3/SM4 国密算法，可提供基于硬件的数据加密保护

桌面环境

文件管理器

- 默认显示相对日期，允许用户切换到绝对日期
- 新增拷贝剩余时间
- 新增支持搜索结果动态更新
- 优化批量拷贝文件效率
- 优化文件管理器磁盘卸载功能
- 新增支持多个文件批量设置只读、隐藏
- 新增用户名和密码的输入框增加工作组 workgroup 的输入框
- 新增支持能够保存账号密码实现自动认证登录的功能
- 新增支持单次认证成功后不重复认证
- 软件保存文件记录上一次位置

设置

- 新增支持蓝牙 AAC/SBC 音频编码切换
- 新增电量低于 1%(可设置)自动待机
- 新增支持普通策略中设置策略优化
- 优化设置-关于界面协议跳转至用户手册对应界面，统一内容显示
- 新增麒麟工作空间页面，控制麒麟工作空间的开关
- 新增设置-关于界面支持光标复制版本信息

- 优化开机自启动应用配置流程
- 优化设置-背景(及锁屏)-线上图片的刷新与显示机制

显示器

- 新增多用户下亮度调节、功耗模式状态同步
- 新增用户共用显示器配置
- 优化显示器配置命名
- 新增指定主屏 （默认将本地大屏接口设置为 0，HDMI 外接口设置为 1）

任务栏

- 优化任务栏应用数量过载时，界面显示

鼠标

- 优化规范命名“双击间隔时长”，“鼠标加速”，“光标”，“光标速度”，“双击速度”提示测试效果，“按 Ctrl 键显示指针位置”优化强调样式，“光标闪烁速度”增加预览

登录与锁屏

- 新增 wps 播放、腾讯会议、ssh、影音播放视频，不会进入锁屏与休眠
- 新增用户加域成功后屏蔽用户操作中的切换用户功能
- 新增系统登录界面和锁屏界面上的时间支持自定义设置是否显示
- 新增桌面锁屏页面网络、键盘、关机隐藏接口
- 新增睡眠/休眠唤醒后需要密码及唤醒屏幕时需要密码管控接口
- 新增锁屏防崩溃机制

声音

- 新增支持蓝牙 AAC/SBC 音频编码切换

软件商店

- 新增软件商店客户端一键返回客户端顶部功能

系统应用

麒麟管家

- 新增支持监控日志目录和磁盘状态，异常时提示用户清理
- 新增系统瘦身支持查找重复文件并清理
- 新增百宝箱搜索功能
- 百宝箱新增修复企业微信、修复 WPS、修复 QQ、修复打印机添加失败、修复 dpkg 无法使用、修复输入法、修复软件安装器、修复微信启动慢小工具

看图

- 新增图片加载提示
- 优化图片目录显示顺序，与文件管理器目录一致

音乐

- 新增显示歌词功能

截图

- 优化截图图片分辨率与缩放率

归档管理器

- 新增打包压缩方式
- 新增支持解压后默认生成与压缩包同名的文件夹

备份还原

- 新增备份阶段断点续传以及随时中断备份的能力
- 新增系统升级进度信号优化，升级过程更平滑

AI 应用

AI 助手

- 新增知识处理引擎，能够快速准确地理解用户提出的各类知识类问题，并依据强大的云端及端侧模型进行精准解答

- 新增快捷操作悬浮条，快捷键唤醒，以直观的悬浮条形式呈现常用操作选项，方便用户随时快速调用，提升操作效率
- 新增指令调度中心，系统指令调用，高效理解和协调各类系统指令，确保系统调用便捷高效
- 新增语音控制中枢，集中处理用户的语音指令，通过先进的语音识别和解析技术，实现便捷的语音交互操作

记忆地图

- 新增时间轴历史记录溯源，以秒级精度构建可视化时间链，自动标记用户各时段激活的前台程序（包含但不限于文件资源管理器、多类型浏览器、生产力工具等）
- 新增 OCR 识别，采用光学字符识别技术实现精准文本复原，跨语言识别，支持中英日法等多语种文字

数据管家

- 新增智能空间，通过智能算法对数据进行分类、整理和优化存储，帮助用户高效管理数据资源，提升数据检索和使用的便捷性，同时确保数据的安全性和隐私保护
- 新增文件映射，将分散在不同存储位置或系统中的文件进行关联和统一管理，确保用户能够快速定位和调用所需文件，提升工作效率
- 新增意图识别，通过自然语言处理和机器学习技术，精准理解用户的操作意图，自动推荐相关数据或执行相应操作，帮助用户更高效地完成数据处理任务
- 新增动态聚合，实时收集、整合来自多个数据源的数据，并根据用户需求进行动态分析和展示，帮助用户快速获取全面、准确的信息支持决策

智能模糊搜索

- 新增向量化搜索，通过将文本数据转化为高维向量，利用向量空间中的相似度计算实现高效、精准的搜索匹配
- 新增自然语言搜索，支持用户以日常语言提问，系统通过语义理解与上下文分析，提供符合意图的搜索结果

麒麟速记

- 新增全场景唤起快速录入，麒麟速记支持快捷键快速唤起，让用户在任何场景下都能迅速启动录入模式，无需繁琐的操作步骤，即可随时随地记录灵感和重要信息
- 新增记录待办或笔记，应用提供了强大的待办事项和笔记功能，用户可以轻松创建、分类和管理各类任务和笔记。无论是工作中的重要事项还是生活中的点滴感悟，都能得到妥善记录和整理
- 新增周报视图，麒麟速记特别设计了周报视图，用户可以每周对过去的工作和生活进行回顾和总结。通过直观的数据分析和图表展示，帮助用户清晰了解自己的工作进度和成果，为下一周的工作提供有力的参考

系统安全

安全中心

- 新增漏洞修复，增加漏洞库更新功能、漏洞扫描功能、漏洞查询功能，联动更新完成漏洞修复功能
- 新增可信度量，兼容支持飞腾、兆芯、海光架构
- 新增网络保护改为防火墙与网络保护，网络模式切换不跳转设置，在防火墙界面完成；

文件保护箱

- 新增支持透明加密保护箱
- 新增支持保护箱导入导出
- 新增支持自动锁定：定时锁定，可配置定时时间，支持注销、锁屏时自动锁定
- 新增支持锁定、注销时清除文管里保护箱文件访问记录
- 优化密码复杂度提示、防暴力破解
- 优化备份还原机制

磁盘加密

- 新增支持磁盘分区加密、取消加密、解锁、锁定
- 新增支持磁盘加密密钥管理，支持通过备份密钥重置密码

- 新增加密密码支持复杂度配置，支持防爆力破解

系统激活

- 新增支持跨架构激活
- 新增适配 BIOS 固件，系统重装之后保持激活状态
- 新增调整硬件信息绑定顺序，保障更换硬盘保持激活状态
- 新增激活客户端支持取消激活
- 新增场地授权激活方式增加时间限制
- 新增 Ukey 激活数据加密

系统更新

- 新增本次升级预估完成时间提示，降低用户升级过程等待焦虑感
- 优化用户交互提示语，提供对用户更加友好的交互体验
- 增加升级故障诊断及修复机制，对于无法修复的问题提供上报机制
- 新增实现轻量级补丁回退机制，支持升级前自动备份及相关自定义配置
- 优化鲁棒性全面提升，实现升级源隔离管理、依赖修复等机制

Kylin SDK 2.5

- 优化拓展电源管理，网络，蓝牙，显示，性能监控等模块；Win32 模块覆盖度从 10%提升到 25%
- 新增 ukui-shell、ukui-window-management、ukui-blur 等协议适配
- 新增接口访问控制
- 新增统一配置模块管理机制，支持可叠加配置、统一化管理应用/用户配置
- 新增 AI 能力，对外提供基础 AI 能力和生成式 AI 能力接口，包括文本、语音、视觉处理等
- 优化发布图形化打包工具，降低软件适配时打包过程的上手难度

通用设置

- 增加 AI 模块管理

系统问题修复

声音

- 修复特定情况下，输入设备设置为模拟耳机之后，无法切换成其他输入设备问题
- 修复声音输入设置为蓝牙耳机后，应用的声音输出设备无法从其他设备切换成蓝牙设备问题
- 修复不插入设备直接对笔记本输入时，录音有较大杂音问题
- 修复调节声音时出现闪退现象问题
- 修复前置 MIC 口插入三段式麦克风，声音输入设备显示为后麦克风（USB Audio）问题

网络

- 修复从任务栏断开 WPA3 无线局域网时卡顿问题
- 修复多次关闭/开启有线网络时，会有短暂卡顿问题
- 修复快捷键关闭 WiFi，重启机器后，需要点击两次才能开启 WiFi 问题
- 修复偶发网络延时问题问题
- 修复偶发桌面系统反复断网问题
- 修复桌面系统网络设置禁掉网卡后依旧能上网问题

系统应用

影音

- 修复标题栏 mini 按钮为空问题
- 修复播放视频只有声音没有画面问题
- 修复播放进度条悬停窗口无预览内容问题

音乐

- 修复声量调节框带有黑色边框显示问题
- 修复 125%缩放率精简模式的音乐界面图标异常问题

- 修复打开音乐歌词弹窗，弹窗歌词显示不全问题
- 修复列表歌词顶部缺少回收按钮问题

看图

- 修复相册中切换图片没有加载提示问题
- 修复图片加载过程中无法操作窗口三联按钮，不能进行最大化/最小化/关闭问题
- 修复修改文管中文件排序方式，看图浏览顺序未能随文管排序变化问题

麒麟管家

- 修复日志异常的通知提示无取消按钮问题
- 修复网络丢包率无法检测出异常问题
- 修复关键库检测异常后无法进行修复问题
- 修复光标在部分小工具的三联按钮及标题栏处样式错误问题
- 修复百宝箱小工具快捷方式不随系统语言改变问题

打印机

- 修复添加打印机时，鼠标悬停下拉箭头时，箭头标志消失问题
- 修复经典打印机入口未适配藏文问题

扫描

- 修复蒙古文下扫描多出文字显示不全问题
- 修复繁体适配翻译不准确问题

刻录

- 修复 ISO9660 文件系统格式的 win 兼容问题
- 修复内外置光驱均无法识别 DL 光盘问题
- 修复内置光驱 DL 格式光盘 ISO9660 格式追加刻录失败问题
- 修复 UDF 格式 RW 盘追加刻录过程中，右键文件管理器侧边栏的光盘卡顿问题
- 修复数据加载过程中拔掉光驱，应用闪退问题
- 修复光盘未加载完毕前关闭刻录会生成 core 文件问题

- 修复两张非空光盘在刻录软件内显示光盘内容与所选光盘不一致问题
- 修复刻录与文管内光盘已使用容量与实际不符问题

归档管理器

- 修复文件打包不压缩后的文件大小与正常压缩后的文件大小相同问题
- 修复压缩 tar.gz 格式的文件异常问题
- 修复系统升级完成后，解压缩到无法弹出文件管理器问题

截图

- 修复卸载看图后，截图也会一并被卸载掉问题

系统安全

安全中心

- 修复防火墙规则存在特殊字符不能修改问题
- 修复病毒防护-扫描的风险项默认没有勾选问题
- 修复设备名称存在特殊字符不能添加放行问题

文件保护箱

- 修复藏文和蒙文下，文件保护箱新建秘钥窗口内容显示不全问题
- 修复偶发文件保护箱文件丢失，需要找回的问题

文件管理器

- 修复点击文件管理器中的 “关于” 选项，软件闪退；点击日志查看器中的 “关于” 选项，软件自动关闭退出；点击工具箱中的 “关于” 选项，软件自动退出问题
- 修复消息弹窗中，点击查看详情按钮，打开页面失败问题
- 修复 txt 文本文档基于文件管理器无法预览问题

桌面环境

- 修复硬件锁飞行模式硬件锁不生效问题
- 修复设置-触控板开关不随快捷键禁用触控板而禁用问题
- 修复注销后登录桌面缓冲时间达 10 秒问题

- 修复登录界面进行休眠会出现闪烁两次登录界面问题
- 修复 Type-C 扩展坞接入显示器，重启后任务栏消失问题

系统更新

- 修复更新环境存在依赖问题时，卸载应用修复报未知错误问题
- 修复单个更新时存在依赖问题需要卸载的有重要和非重要软件包，更新失败时没有错误码问题
- 修复更新系统后，打开微信提示权限问题问题
- 修复系统更新包下载完成后提示预估安装时间为 0 分钟问题
- 修复在线更新时升级失败再次检测无法获取到升级信息问题
- 修复在线更新偶发激活丢失问题
- 修复安全中心修复漏洞安装失败导致更新功能不可用问题

其他修复内容

浪潮

CE720F2

- 系统时间与 bios 时间不一致
- 按下电脑电源键，不弹出电源菜单

天熠

TR31A1

- 双屏显示异常
- 调节使用电源时电源计划，CPU 当前使用率未发生变化
- 使用 line in 线和手机/电脑设备连接，手机/电脑设备播放声音，输入音量无反馈

TR11B0

- 设置-鼠标-指针大小选择最大，指针闪烁或消失不见
- 设置-显示器未有亮度调节设置框
- HDMI 声音输出声音异常卡顿

长城

TA238A2

- 连接双屏扩展模式下，一体机显示器屏幕会闪烁几次
- 显卡未适配 4K 屏
- 使用 line in 线和手机/电脑设备连接，手机/电脑设备播放声音，输入音量无反馈

TN140A2

- 显示器亮度调节失败
- Type-C 扩展坞扩展坞接入显示器不亮
- 硬件锁飞行模式硬件锁不生效

TD120A2

- 人脸录入提示打开设备失败
- 按下电源键，不弹出关机菜单
- 连接 4k 屏，切换 4k 分辨率，黑屏一段时间后切换回原分辨率

宝德

PT620K

- 机器无睡眠模式
- 不支持 25hz 的分辨率
- 不支持 1280*1024、1024*768、1152*864 的分辨率
- gfortran 和 g++安装完以后，执行命令找不到，使用 KylinPVT 工具跑 speccpu 跑出来的数据不完全
- 插入 usb 耳机，桌面右下角显示声音图标；拔掉 usb 耳机，桌面右下角显示耳机图标
- 播放视频时注销，测试过程中插拔主屏和副屏，登录界面会变成镜像模式

PT620Q

- 音量输出设备为 USB 耳机，睡眠唤醒后，音量输出设备改变
- 输入输出是 3.5mm（三段式）双孔耳机，录音时无音量反馈，录制的音频全为噪音

升腾

P410-2

- 内存制造商显示 unknown

- 扩展模式下切换非 4K 屏分辨率，4k 屏边缘处概率出现部分花屏
- 扩展模式下切换非 4K 屏分辨率，点击不保存，4k 屏右侧边缘处出现黑条
- 音频输入插入 Line-in 线后有音量反馈但音量条置灰
- Line-in 线录制声音最大音量时存在部分杂音
- 连接双屏，更改分辨率时，4K 屏会有黑块或花屏
- S4 1000 次稳定性测试执行失败
- 默认安装的系统睡眠后无法用键盘鼠标唤醒，执行研发提供的脚本后睡眠自动唤醒
- 播放.ts 格式视频花屏

D410

- 平衡模式切节能模式，CPU 使用率没有明显降低，反而有所升高
- 声音输入输出无法识别 typec 耳机
- 硬盘接口类型显示错误
- 设备无光驱但是光驱检查不为空
- Type-C 扩展坞接 HDMI 和 VGA 均不亮

P410

- S3 1000 次测试失败，且网络服务被关闭
- reboot500 次过程中黑屏
- speccpu 执行结果不全

W710

- 没有适配 4k 的分辨率
- 机器使用一段时间后，发现休眠功能丢失
- 登录界面进行休眠会出现闪烁两次登录界面
- Type-C 扩展坞上接入的 HDMI 和 VGA 显示器不亮

天阔

N40

- 执行睡眠后无法唤醒
- 笔记本合盖后再次打开黑屏

- 系统使用一段时间后蓝牙模块消失

联想

N80N

- 无法识别到蓝牙，安全中心重新放行后蓝牙功能可用
- 无法获取到触摸板信息
- 接入 4k 屏，笔记本屏幕设置为副屏，任务栏时间一直抖动
- Type-C 扩展坞接入显示器不亮
- 测试机使用 line in 线和手机/电脑设备连接，手机/电脑设备播放声音，录制的音频无声音
- 副屏修改方向后，主屏被拉长

X1

- S4 1000 次稳定性测试失败
- Type-C 扩展坞接入显示器，重启后任务栏消失

M70Z

- 开机过程麒麟 logo 分辨率异常

N80z

- 打开飞行模式后再关闭，无线网开关打开
- 拔出某个声音输出设备再插入，声音变为从低优先级的扬声器输出
- S3 1000 次稳定性测试电脑死机
- S4 1000 次稳定性测试执行失败
- 工具箱中显示的 bios 厂商与 bios 中不一致

M710

- 机器使用一段时间后，发现休眠功能丢失
- S4 1000 次稳定性测试执行失败
- 工具箱中显示的 bios 厂商与 bios 中不一致

GeekPro-14

- 休眠概率黑屏卡死
- 稳定性测试概率性黑屏或黑屏仅剩鼠标

- 满载外设 S3/S4 混合测试 300 次黑屏
- 开安全后 netperf 测试性能劣化超 5%
- netperf 测试性能对比 uos 劣化超 5%

m435

- 满载外设 S3/S4 混合（300 次）失败，黑屏卡死
- 稳定性测试概率性黑屏或黑屏仅剩鼠标
- 第一次开机登录后没有自动播放新功能介绍动画

华为

Mate14

- 不识别机器板载输入输出设备
- 不识别 3.5mm 耳机
- 任务栏调节音乐和影音的声音无效
- 无法识别到蓝牙模块

惠普

440G7

- 重启概率提示重复登录，无法进入桌面

440G8

- reboot 稳定性测试概率性提示：当前用户已经在系统中登录!目前系统不支持同时登录一个以上相同用户下方按钮退出

附录 修复的 CVE 安全漏洞清单

在所有平台上修复的 CVE 清单

CVE-2023-38633 、 CVE-2021-46848 、 CVE-2021-30475 、 CVE-2021-30474 、 CVE-2021-30473 、 CVE-2018-13876 、 CVE-2018-13870 、 CVE-2018-13872 、 CVE-2018-13874 、 CVE-2018-13869 、 CVE-2018-13868 、 CVE-2022-33065 、 CVE-2023-6186、CVE-2023-6185、KVE-2023-1214、KVE-2023-1215、KVE-2023-1216、

CVE-2024-2961 、 CVE-2024-4453 、 CVE-2024-33601 、 CVE-2024-33599 、
CVE-2024-33600 、 CVE-2024-33602 、 CVE-2023-0996 、 CVE-2023-29659 、
CVE-2020-23109 、 CVE-2024-40767 、 CVE-2024-32230 、 CVE-2024-41810 、
CVE-2024-41957 、 CVE-2024-43374 、 CVE-2024-6923 、 CVE-2024-6232 、
CVE-2024-8088 、 CVE-2023-27043 、 CVE-2024-7592 、 CVE-2024-7592 、
CVE-2024-39331 、 CVE-2024-30205 、 CVE-2024-30203 、 CVE-2023-28617 、
CVE-2022-48339 、 CVE-2024-30204 、 CVE-2022-48337 、 CVE-2022-45939 、
CVE-2024-45751 、 CVE-2024-7788 、 CVE-2024-45614 、 CVE-2023-46589 、
CVE-2024-24968 、 CVE-2024-23984 、 CVE-2024-47176 、 CVE-2023-39327 、
CVE-2023-49582 、 CVE-2023-26112 、 CVE-2024-42472 、 CVE-2019-10190 、
CVE-2019-10191 、 CVE-2020-12667 、 CVE-2019-19331 、 CVE-2024-43802 、
CVE-2023-27043 、 KVE-2024-1001 、 CVE-2021-43177 、 CVE-2024-8796 、
CVE-2023-48795 、 CVE-2024-3596 、 CVE-2024-36474 、 CVE-2024-42415 、
CVE-2021-38578 、 CVE-2022-0204 、 CVE-2024-5742 、 CVE-2022-36227 、
CVE-2023-31315 、 CVE-2024-8508 、 CVE-2024-9632 、 CVE-2024-37891 、
CVE-2024-20696 、 CVE-2021-3575 、 CVE-2021-29338 、 CVE-2022-1122 、
CVE-2024-10573 、 CVE-2023-3019 、 、 CVE-2024-21210 、 CVE-2024-21217 、
CVE-2024-21235 、 CVE-2024-21208 、 CVE-2024-21210 、 CVE-2024-21235 、
CVE-2024-21208 、 CVE-2024-21217 、 CVE-2024-46953 、 CVE-2024-46951 、
CVE-2024-46955 、 CVE-2024-46956 、 KVE-2024-1101 、 KVE-2024-1102 、
CVE-2024-21212 、 CVE-2024-21201 、 CVE-2024-21199 、 CVE-2024-21213 、
CVE-2024-21236 、 CVE-2024-21197 、 CVE-2024-21219 、 CVE-2024-21193 、

CVE-2024-21237 、 CVE-2024-21231 、 CVE-2024-21239 、 CVE-2024-21196 、
CVE-2024-21194 、 CVE-2024-21198 、 CVE-2024-21230 、 CVE-2024-21241 、
CVE-2024-3772 、 CVE-2023-29405 、 CVE-2023-24531 、 CVE-2024-24791 、
CVE-2023-39325 、 CVE-2023-45288 、 CVE-2024-24783 、 CVE-2023-29406 、
CVE-2023-39318 、 CVE-2023-45290 、 CVE-2023-39323 、 CVE-2022-41725 、
CVE-2024-34155 、 CVE-2023-29404 、 CVE-2024-24784 、 CVE-2024-24790 、
CVE-2023-29403 、 CVE-2021-40812 、 、 CVE-2023-46445 、 CVE-2023-46446 、
CVE-2024-9287 、 CVE-2024-6232 、 CVE-2024-6923 、 CVE-2024-49769 、
CVE-2024-48991 、 CVE-2024-11003 、 CVE-2024-48992 、 CVE-2024-48990 、
CVE-2024-10224 、 CVE-2023-40889 、 CVE-2023-40890 、 CVE-2024-35176 、
CVE-2024-41946 、 CVE-2024-39908 、 CVE-2024-41123 、 CVE-2024-49761 、
KVE-2024-1112 、 KVE-2024-1113 、 KVE-2024-1201 、 CVE-2024-38517 、
CVE-2024-52533 、 CVE-2024-52530 、 CVE-2024-52531 、 CVE-2024-52532 、
KVE-2024-1106 、 KVE-2024-1109 、 KVE-2024-1203 、 CVE-2024-47814 、
CVE-2024-10978 、 CVE-2024-10979 、 CVE-2024-10977 、 CVE-2024-10976 、
CVE-2021-46021 、 CVE-2019-11637 、 CVE-2019-6456 、 CVE-2019-11640 、
CVE-2021-46022 、 CVE-2019-11639 、 CVE-2019-6455 、 CVE-2019-6459 、
CVE-2019-6460 、 CVE-2021-46019 、 CVE-2019-6458 、 CVE-2019-11638 、
CVE-2019-6457 、 CVE-2024-53907 、 KVE-2024-1111 、 KVE-2024-0603 、
CVE-2022-40468 、 CVE-2021-32719 、 CVE-2021-32718 、 KVE-2023-1208 、
CVE-2023-4233 、 CVE-2023-2794 、 CVE-2023-4234 、 CVE-2023-4235 、
CVE-2023-4232 、 CVE-2024-50602 、 CVE-2024-24968 、 CVE-2024-21820 、

CVE-2024-23984 、 CVE-2024-21853 、 CVE-2024-23918 、 CVE-2023-28447 、
CVE-2018-25047 、 CVE-2024-35226 、 CVE-2024-11233 、 CVE-2024-11236 、
CVE-2024-8929 、 CVE-2024-8932 、 CVE-2024-11234 、 KVE-2024-1206 、
KVE-2024-1205 、 KVE-2025-0101 、 CVE-2024-53849 、 CVE-2023-0341 、
CVE-2024-47606 、 CVE-2024-47542 、 CVE-2024-47600 、 CVE-2024-47541 、
CVE-2024-47607 、 CVE-2024-47615 、 CVE-2024-47835 、 CVE-2024-47538 、
CVE-2022-48560 、 CVE-2023-24329 、 CVE-2022-48566 、 CVE-2023-40217 、
CVE-2022-48565 、 CVE-2024-36617 、 CVE-2021-34121 、 CVE-2021-23206 、
CVE-2021-40985 、 CVE-2021-23191 、 CVE-2021-43579 、 CVE-2021-20308 、
CVE-2021-26259 、 CVE-2021-26252 、 CVE-2021-23158 、 CVE-2021-34119 、
CVE-2021-26948 、 CVE-2023-49606 、 CVE-2024-45338 、 CVE-2024-12085 、
CVE-2024-12088 、 CVE-2024-12087 、 CVE-2024-12086 、 CVE-2024-12747 、
CVE-2021-31315 、 CVE-2021-31317 、 CVE-2021-31320 、 CVE-2021-31318 、
CVE-2021-31321 、 CVE-2021-31319 、 CVE-2021-31322 、 CVE-2020-6923 、
CVE-2023-39929 、 CVE-2019-15903 、 CVE-2022-22824 、 CVE-2022-22822 、
CVE-2022-22823 、 CVE-2022-22825 、 CVE-2022-22826 、 CVE-2018-20843 、
CVE-2016-4472 、 CVE-2022-22827 、 CVE-2016-0718 、 CVE-2021-46143 、
CVE-2015-1283 、 CVE-2024-56374 、 CVE-2020-17482 、 CVE-2022-27227 、
CVE-2022-27227 、 CVE-2020-14954 、 CVE-2020-28896 、 CVE-2021-32055 、
CVE-2022-1328 、 CVE-2024-49393 、 CVE-2024-49394 、 CVE-2024-56378 、
CVE-2020-11867 、 CVE-2023-44441 、 CVE-2022-42920 、 CVE-2018-11255 、
CVE-2020-18971 、 CVE-2018-20797 、 CVE-2018-12983 、 CVE-2021-30470 、

CVE-2021-30471 、 CVE-2019-10723 、 CVE-2018-8002 、 CVE-2025-22134 、
CVE-2022-0534 、 CVE-2022-24191 、 CVE-2022-27114 、 CVE-2024-45508 、
CVE-2024-46478 、 CVE-2022-0137 、 CVE-2022-28085 、 CVE-2022-34033 、
CVE-2022-34035 、 CVE-2021-33582 、 CVE-2024-56826 、 CVE-2024-56827 、
CVE-2023-50229 、 CVE-2023-50230 、 CVE-2024-53432 、 CVE-2022-46169 、
CVE-2024-55553 、 CVE-2024-44070 、 CVE-2024-12426 、 CVE-2024-12425 、
CVE-2023-27783 、 CVE-2023-4256 、 CVE-2023-27786 CVE-2023-27788 、
CVE-2023-27784 、 CVE-2023-27789 、 CVE-2023-27785 、 CVE-2023-43279 、
CVE-2023-27787 、 CVE-2024-12705 、 CVE-2024-11187 、 CVE-2024-34459 、
CVE-2022-49043 、 CVE-2020-11022 、 CVE-2020-11023 、 CVE-2024-56201 、
CVE-2024-56326 、 CVE-2024-46461 、 CVE-2023-25193 、 CVE-2023-22497 、
CVE-2025-21502 、 CVE-2024-24816 、 CVE-2022-24728 、 CVE-2023-28439 、
CVE-2024-24815 、 CVE-2024-36293 、 CVE-2024-39279 、 CVE-2024-31068 、
CVE-2024-12133 、 CVE-2023-51698 、 CVE-2024-53899 、 CVE-2024-13176 、
CVE-2024-9143 、 CVE-2025-1390 、 CVE-2025-23419 、 CVE-2022-24823 、
CVE-2024-29025 、 CVE-2025-24928 、 CVE-2025-27113 、 CVE-2024-56171 、
CVE-2023-48795 、 CVE-2024-48651 、 CVE-2023-51713 、 CVE-2024-47887 、
CVE-2024-41128 、 CVE-2024-47889 、 CVE-2024-47888 、 CVE-2012-1148 、
CVE-2024-52006 、 CVE-2024-50349 、 CVE-2024-45409 、 CVE-2022-39209 、
CVE-2023-26485 、 CVE-2023-22486 、 CVE-2025-25471 、 CVE-2025-25473 、
CVE-2025-25469 、 CVE-2025-22921 、 CVE-2025-25468 、 CVE-2025-22919 、
CVE-2025-22920 、 CVE-2025-26618 、 CVE-2005-1794 、 CVE-2023-27372 、

CVE-2024-8517 、 CVE-2023-24258 、 CVE-2024-0321 、 CVE-2024-46981 、 CVE-2024-31228 、 CVE-2020-1739 、 CVE-2025-26699 、 CVE-2024-10525 、 CVE-2025-1080、CVE-2025-24813