



银河麒麟桌面操作系统 V10 SP1 2403  
版本发布说明

麒麟软件有限公司

2024 年 4 月

## 整体概述

银河麒麟桌面操作系统 V10 SP1 2403 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、海光 2 号、海光 3 号、海光 C86-4G、兆芯 zx-c+、兆芯开先系列（KX-7000、KX-6000G、KX-6000、KX-5000）、兆芯 KH-40000 系列、申威 831、kirin 990、kirin 9006C、kirin M900、kirin 9000C，支持 Intel 最新 12、13 代酷睿处理器和最新的 AMD 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 2303，银河麒麟桌面操作系统 V10 SP1 2403 变更模块主要包括：

- **新增功能及优化：**新硬件支持，系统启动，系统语言，桌面环境（文件管理器、电源管理、任务栏、账户、登录、网络、声音、显示、触控），软件商店，系统应用（归档管理器、用户手册、备份还原），系统安全，系统性能，系统激活，系统更新，Kylin SDK 2.3，安全管控 4.0；
- **系统问题修复：**系统安装，桌面环境（文件管理器、任务栏、全局搜索、窗口管理器、侧边栏、账户、显示、声音、网络、录音、多屏协同、电源），系统应用（影音、音乐、麒麟管家、归档管理器、看图、刻录、安装器），系统安全（安全中心、文件保护箱），软件商店、系统更新。
- **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 2303	V10 SP1 2403
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）	2.31、2.28（SW831、龙芯 3A5000、3A6000）
gcc	9.3.0、8.3.0（龙芯 3A5000）	9.3.0、8.3.0（龙芯 3A5000、3A6000）
qt	5.12.12	5.12.12、4.8.7
gtk	2.24、3.24	2.24、3.24

systemd	245	245
---------	-----	-----

## 新增功能和特性

### 新硬件支持

#### CPU

- 新增支持龙芯 3A6000 处理器
- 新增支持飞腾 D3000 处理器
- 新增支持兆芯 KX-7000 处理器
- 新增支持海光 C86-4G

#### GPU

- 新增支持 709 GP201 显卡
- 新增支持芯瞳 GB2062 显卡
- 申威新增 SM768 显卡支持
- 龙芯新增象帝先天钧一号驱动支持

#### 网卡

- 新增支持苏州速通 SCM2625 无线网卡

### 内核

- 支持 LMK 机制，保护核心进程、
- 支持海光 HCT 功能
- 支持海光 CSV2 虚拟机
- 增加 Android LMK 技术，保护核心进程
- 申威平台 KGDB 调试工具调优
- 支持可信驱动 TPM2.0、TCM1.0

## 桌面环境

### 文件管理器

- 文件列表排序增加“创建时间”属性
- 系统文件搜索大文件时的速度提升
- 文件管理器提供个人文件夹显示隐藏接口
- 支持扩展插件管理和配置，自研或第三方插件的启用、禁用开关

### 系统语言

- 新增支持蒙古文、繁体

### 任务栏

- 提供任务栏隐藏关机/重启/注销/切换用户/睡眠按钮的接口

### 账户

- 支持纯数字用户名

### 登录

- 人脸解锁耗电优化

### 网络

- 支持拨号上网功能

### 声音

- 增加应用可选择不同设备播放的功能
- 音频设置界面增加设备禁用功能与接口

### 显示

- 支持色温可随日出日落自动调节

### 触控

- 增加触摸板开关选项

## 电源

- 增加屏幕光感功能
- 新增支持快速开合盖功能

## 远程桌面

- 远程桌面要求用户输入的密码密文保存

## 软件商店

- 软件商店客户端更新
- 任务栏中软件商店应用更新增加红点提示

## 系统应用

### 归档管理器

- 归档管理器支持剪切操作

### 用户手册

- 支持用户手册文本选中和复制

### 备份还原

- 系统备份压缩优化，备份速度提升

## 系统安全

### 安全中心

- 昆仑固件安全启动
- 可信驱动更新适配
- 优化防火墙规则命名，减少防火墙频繁弹框
- 升级 Kysec v1.5，优化应用程序执行控制
- 安装软件一定时间内只需要输入一次密码

### 系统激活

- 支持获取终端 MAC 地址或其它能够识别设备的加密信息

- KMS 激活支持服务端和客户端端口自定义
- 支持服务续期后系统服务有效期联网自动更新
- 支持压缩格式的授权文件导入
- 支持部分整机商联网自动激活
- 支持关键硬件未更换时重装系统后联网自动激活

## 系统更新

- 增加更新前版本补丁匹配检测机制
- 支持用户升级体验计划，用户手动上报错误日志

## Kylin SDK 2.3

- 安全 SDK 扩展，优化外设管控，新增用户账户管理、登录认证等 API
- 完善 SDK 开发文档，完善 web、桌面应用、驱动、安全应用开发指导文档

## 安全管控 4.0

- 全面提升了用户管理、终端管理、组织管理、任务管理、软件管理、策略管理、服务器管理、系统管理、同步与级联、日志与报表、对外接口、高可用、加域、退域等模块能力

# 系统问题修复

## 系统安装

- 修复藏文安装过程中文字显示不全问题
- 修复部分情况下双磁盘加密安装系统后，登录界面无法登录进入系统问题
- 修复接入网线，安装完成界面会弹出网络弹窗问题
- 修复部分机器 U 盘安装后重启偶现系统黑屏问题
- 修复安装过程中，展开再收回安装日志时宣传图片闪动问题
- 修复正在安装界面，滚动介绍页中软件商店的介绍文字有误问题
- 修复安装过程中，展开再收回安装日志时宣传图片闪动问题

## 桌面环境

### 文件管理器

- 修复勾选文件为隐藏时文件不能立即隐藏问题
- 修复选中文件的状态下，拖拽文件管理器界面文件选中状态闪烁问题
- 修复偶现文件重命名复制粘贴失败的问题
- 修复删除 3W+文件，界面响应时间超过 3s 问题
- 修复连接服务器页面添加个人收藏服务器失效问题
- 修复关闭文件管理器时插入异常 U 盘，侧边栏没有 U 盘图标问题
- 修复从数据盘删除文件至回收站，再从回收站复制该文件至桌面，文件名称带路径问题

### 任务栏

- 修复应用悬浮弹窗点击后不消失问题
- 修复打开应用，点击任务栏预览框关闭按钮，任务栏概率性崩溃的问题问题
- 修复右键点击任务栏应用图标后概率性任务栏消失问题
- 修复移动托盘中的图标后，鼠标会变成十字光标问题

### 全局搜索

- 修复偶现无法搜到任何设置项问题

### 窗口管理器

- 修复打开任意应用后，偶现无法进入多任务视图界面问题
- 修复鼠标悬停任务栏缩略图关闭后，桌面其他应用窗口消失问题

### 侧边栏

- 修复修改时间格式为 12 小时侧边栏闪退问题

### 账户

- 修复多用户自动登录失败，提示弹窗无法关闭、控制面板无法操作问题

## 显示

- 修复重启后连接列表中任意网络显示器，远端无弹窗弹出，连接失败问题
- 修复切换多屏显示为笔记本屏幕后侧边栏调节夜间模式，控制面板闪退问题

## 声音

- 修复输出设备处无法检测到蓝牙输出设备问题

## 网络

- 修复 wifi 使用过程中经常性出现界面卡顿, 托盘图标消失问题
- 修复应用代理异常，设置代理后无法正常连接网络问题
- 修复 PPTP VPN 连接失败问题

## 录音

- 修复插拔耳机后，录音会自动停止问题

## 多屏协同

- 修复手机投屏连接后，pc 端投屏界面显示黑屏问题

## 电源

- 修复睡眠唤醒后、应用被关闭，网络概率性无法连接需要重启的问题

## 系统应用

### 影音

- 修复切换解码器设置 2 次后，影音概率性闪退问题

### 音乐

- 修复播放视频过程中休眠，唤醒后视频出现卡顿、闪屏现象问题
- 修复双击列表中源文件被删除的音乐，应用闪退问题

### 麒麟管家

- 修复偶现打开应用的响应速度太慢问题



## 归档管理器

- 修复加密文档无法解压到自定义路径问题

## 看图

- 修复打开大 BMP 图片无法正常显示问题
- 修复另存为-exr 图片另存为其它图片格式，保存后的图片显示异常问题

## 刻录

- 修复 UDF 格式光盘追加刻录长名称文件夹后，无法续刻问题

## 安装器

- 修复安装未签名软件 5 分钟后再次安装未签名软件不需要输入密码问题
- 修复关于界面文字未翻译问题

## 系统安全

### 安全中心

- 修复文件访问权限控制目录设置为允许，部分应用仍提示无权限问题
- 修复卸载软件后，安全中心病毒防护界面置灰问题
- 修复插入安全内存条，安全中心未识别安全内存问题

### 文件保护箱

- 修复通过文件管理器无法创建、卸载、删除、重命名文件保护箱问题

## 软件商店

- 修复更新源后，软件商店内容为空，且搜索框输入内容应用会闪退问题

## 系统更新

- 修复第二次检测更新未显示待更新应用列表问题
- 修复单个更新软件包到安装阶段后取消按钮未置灰问题
- 修复升级前后分辨率、刷新率不一致问题

## 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-2023-38497、CVE-2023-37920、CVE-2022-25315、CVE-2022-23304、CVE-2022-23303、  
CVE-2022-22823、CVE-2022-22824、CVE-2022-22822、CVE-2021-1871、CVE-2021-1870、CVE-2020-9895、  
CVE-2020-13753、CVE-2020-9850、CVE-2020-10018、CVE-2019-8375、CVE-2018-1999010、  
CVE-2018-12911、CVE-2018-13871、CVE-2018-13866、CVE-2018-13867、CVE-2017-17821、  
CVE-2017-1000121、CVE-2017-5949、CVE-2023-32360、CVE-2020-22219、CVE-2023-20900、  
CVE-2020-21890、CVE-2020-21710、CVE-2020-22628、CVE-2023-4863、CVE-2023-4574、CVE-2023-4584、  
CVE-2023-4575、CVE-2023-4581、CVE-2023-4573、CVE-2023-4504、CVE-2020-22218、CVE-2021-42717、  
CVE-2023-24021、CVE-2022-48279、CVE-2023-4863、CVE-2023-41164、CVE-2020-22217、CVE-2020-8265、  
CVE-2020-8287、CVE-2020-8174、CVE-2023-3341、  
CVE-2022-48541、CVE-2023-44488、CVE-2023-5217、CVE-2023-43786、CVE-2023-43789、CVE-2023-43788、  
CVE-2023-43787、CVE-2023-43785、CVE-2023-43787、CVE-2023-43786、CVE-2023-5176、CVE-2023-4580、  
CVE-2023-5169、CVE-2023-4577、CVE-2023-5171、CVE-2023-5217、CVE-2023-3600、CVE-2023-4585、  
CVE-2023-4578、CVE-2023-4583、CVE-2023-4057、CVE-2023-4692、CVE-2023-4693、  
CVE-2023-39351、CVE-2023-40186、CVE-2023-40569、CVE-2023-40589、CVE-2023-39354、  
CVE-2023-40181、CVE-2023-39353、CVE-2023-39350、CVE-2023-40188、CVE-2023-40567、  
CVE-2023-43665、CVE-2021-22883、CVE-2021-22884、CVE-2023-36328、CVE-2021-41183、  
CVE-2022-31160、CVE-2021-41184、CVE-2021-41182、CVE-2023-43641、CVE-2021-37706、  
CVE-2022-39244、CVE-2022-31031、CVE-2021-43301、CVE-2022-23608、CVE-2022-24793、  
CVE-2022-23537、CVE-2021-43299、CVE-2022-24763、CVE-2022-24764、CVE-2021-43845、  
CVE-2022-21722、CVE-2021-43804、CVE-2021-43300、CVE-2021-43303、CVE-2022-217239、  
CVE-2022-3591、CVE-2022-3352、CVE-2022-3234、CVE-2022-4293、CVE-2022-3520、CVE-2022-3256、  
CVE-2022-3705、CVE-2022-4292、CVE-2022-3324、CVE-2023-4091、CVE-2023-42669、CVE-2023-4154、  
CVE-2023-38546、CVE-2023-1916、CVE-2020-22040、CVE-2020-22051、CVE-2020-22043、CVE-2020-22039、  
CVE-2020-22024、CVE-2021-38090、CVE-2021-38093、CVE-2022-48434、CVE-2021-38092、  
CVE-2020-22038、CVE-2021-38094、CVE-2021-38091、CVE-2020-20898、CVE-2023-32307、CVE-2023-1002、  
CVE-2023-5367、CVE-2023-5380、CVE-2023-3446、CVE-2023-3817、CVE-2023-22079、CVE-2023-22066、  
CVE-2023-22114、CVE-2023-22112、CVE-2023-22059、CVE-2023-22068、CVE-2023-22070、  
CVE-2023-22103、CVE-2023-22084、CVE-2023-22032、CVE-2023-22097、CVE-2023-22092、  
CVE-2023-22064、CVE-2023-22078、CVE-2022-29501、CVE-2022-29500、CVE-2023-34059、  
CVE-2023-34058、CVE-2020-4044、CVE-2023-40743、CVE-2023-5724、CVE-2023-5730、CVE-2023-5732、  
CVE-2023-5721、CVE-2023-5728、CVE-2023-5725、CVE-2023-36054、CVE-2023-45803、CVE-2023-43804、  
CVE-2020-35357、CVE-2022-23468、CVE-2022-23477、CVE-2022-23479、CVE-2022-23484、  
CVE-2022-23481、CVE-2022-23493、CVE-2022-23480、CVE-2022-23483、CVE-2022-23478、  
CVE-2023-42822、CVE-2022-23482、CVE-2023-40184、CVE-2022-4254、CVE-2023-46316、CVE-2023-4016、  
CVE-2021-38090、CVE-2021-38093、CVE-2022-48434、CVE-2021-38092、CVE-2020-22038、  
CVE-2021-38094、CVE-2021-38091、CVE-2020-20898、CVE-2021-33391、CVE-2022-37032、  
CVE-2023-46753、CVE-2023-45803、CVE-2023-43804、CVE-2023-23583、CVE-2023-1672、CVE-2023-38469、  
CVE-2023-38471、CVE-2023-38472、CVE-2023-38470、CVE-2023-38473、CVE-2023-0809、CVE-2021-41039、  
CVE-2023-3592、CVE-2021-34431、CVE-2023-46118、CVE-2023-46848、CVE-2023-46846、CVE-2023-46847、  
CVE-2023-46728、CVE-2023-5981、CVE-2022-32212、CVE-2023-45802、CVE-2023-31122、CVE-2023-44487、  
CVE-2023-3576、CVE-2022-40090、CVE-2013-20001、CVE-2022-37051、CVE-2020-23804、CVE-2022-38349、



CVE-2022-37050、CVE-2022-37052、CVE-2023-40217、CVE-2023-47038、CVE-2023-6206、CVE-2023-6212、  
CVE-2023-6204、CVE-2023-6207、CVE-2023-6209、CVE-2023-6208、CVE-2023-6205、CVE-2023-5366、  
CVE-2023-22067 、 CVE-2022-40433 、 CVE-2023-22081 、 CVE-2023-22025 、 CVE-2023-22081 、  
CVE-2023-22025 、 CVE-2023-22081 、 CVE-2023-22025 、 CVE-2023-40476 、 CVE-2023-44429 、  
CVE-2023-40474 、 CVE-2023-44446 、 CVE-2023-40475 、 CVE-2023-37329 、 CVE-2022-37454 、  
CVE-2022-37454 、 CVE-2023-39352 、 CVE-2023-39356 、 CVE-2022-41877 、 CVE-2022-30067 、  
CVE-2023-44444 、 CVE-2023-44442 、 CVE-2023-44441 、 CVE-2022-32990 、 CVE-2023-44443 、  
CVE-2022-25802 、 CVE-2023-41260 、 CVE-2023-41259 、 CVE-2021-38562 、 CVE-2023-25155 、  
CVE-2022-36021 、 CVE-2022-24834 、 CVE-2023-45145 、 CVE-2023-28856 、 CVE-2022-35977 、  
CVE-2023-45539、KVE-2023-1201、KVE-2023-1202、CVE-2023-49083、CVE-2023-23931、CVE-2023-46219、  
CVE-2023-46218、KVE-2023-1204、CVE-2021-42260、CVE-2023-4806、CVE-2023-4813、  
CVE-2023-45866、CVE-2023-39804、CVE-2023-42464、CVE-2023-28447、CVE-2022-29221、KVE-2023-1208、  
CVE-2023-6377、CVE-2023-6478、CVE-2023-33460、CVE-2017-16516、CVE-2022-24795、CVE-2019-13147、  
CVE-2022-24599、KVE-2023-1209、KVE-2023-1210、CVE-2023-48795、CVE-2023-48795、CVE-2023-51385、  
KVE-2023-1213、KVE-2023-1218、KVE-2023-1220、KVE-2023-1212、KVE-2023-1211、KVE-2023-1217、  
KVE-2023-1221、KVE-2023-1222、CVE-2023-2828、  
CVE-2021-41617、CVE-2023-6859、CVE-2023-6860、CVE-2023-6863、CVE-2023-6858、CVE-2023-6864、  
CVE-2023-6856、CVE-2023-6857、CVE-2023-50762、CVE-2023-6861、CVE-2023-6862、CVE-2023-50761、  
CVE-2022-30333 、 CVE-2023-40477 、 CVE-2022-26563 、 CVE-2022-47008 、 CVE-2022-47011 、  
CVE-2022-47007 、 CVE-2022-47010 、 CVE-2022-45703 、 CVE-2022-44840 、 CVE-2024-21886 、  
CVE-2024-21885、CVE-2024-0408、CVE-2024-0409、CVE-2023-6816、CVE-2024-0229、  
CVE-2023-48795、KVE-2024-0102、CVE-2023-51764、KVE-2024-0103、CVE-2023-50269、CVE-2023-49286、  
CVE-2023-49285 、 CVE-2022-47015 、 CVE-2023-22084 、 CVE-2023-48795 、 CVE-2020-28493 、  
CVE-2024-22195 、 CVE-2023-51766 、 CVE-2023-44271 、 CVE-2023-50447 、 CVE-2020-21606 、  
CVE-2021-36408 、 CVE-2020-21595 、 CVE-2020-21601 、 CVE-2020-21598 、 CVE-2020-21602 、  
CVE-2020-21605 、 CVE-2020-21600 、 CVE-2020-21597 、 CVE-2020-21599 、 CVE-2020-21603 、  
CVE-2020-21596、CVE-2020-21604、CVE-2023-2953、CVE-2024-20973、CVE-2024-20963、CVE-2024-20962、  
CVE-2024-20972 、 CVE-2024-20964 、 CVE-2024-20965 、 CVE-2024-20978 、 CVE-2024-20970 、  
CVE-2024-20981 、 CVE-2024-20976 、 CVE-2024-20966 、 CVE-2024-20960 、 CVE-2024-20982 、  
CVE-2024-20984 、 CVE-2024-20977 、 CVE-2024-20971 、 CVE-2023-30577 、 CVE-2024-21626 、  
CVE-2023-51764、CVE-2023-5678、CVE-2024-0727、CVE-2024-24680、CVE-2022-43242、CVE-2022-43243、  
CVE-2021-36409 、 CVE-2021-36410 、 CVE-2022-43240 、 CVE-2022-43239 、 CVE-2022-43237 、  
CVE-2021-36411 、 CVE-2022-43236 、 CVE-2022-43253 、 CVE-2022-43241 、 CVE-2022-43235 、  
CVE-2021-35452、CVE-2022-43252、CVE-2022-43238、CVE-2022-43248、CVE-2024-1141、CVE-2021-45958、  
CVE-2022-31117、CVE-2022-31116、CVE-2023-4641、CVE-2023-6228、CVE-2023-52356、CVE-2023-6277、  
CVE-2023-50868、CVE-2023-5517、CVE-2023-6516、CVE-2023-4408、CVE-2023-50387、CVE-2023-42282、  
KVE-2024-0201、  
KVE-2024-0203、KVE-2024-0204、KVE-2024-0205、CVE-2022-47665、CVE-2023-24752、CVE-2022-43244、  
CVE-2023-24754 、 CVE-2023-24756 、 CVE-2022-43245 、 CVE-2023-24758 、 CVE-2023-24751  
CVE-2023-25221 、 CVE-2022-43250 、 CVE-2022-43249 、 CVE-2023-24757 、 CVE-2023-24755 、  
CVE-2024-25062、CVE-2023-50387、CVE-2023-50868、CVE-2023-43770、CVE-2022-48624、CVE-2023-6110、  
CVE-2022-48623 、 CVE-2024-24806 、 CVE-2023-50868 、 CVE-2023-50387 、 CVE-2023-29197 、  
CVE-2022-24775、CVE-2024-27351、CVE-2024-26130、CVE-2023-50782、CVE-2023-23920、CVE-2024-0746、  
CVE-2024-0753、CVE-2024-0747、CVE-2024-1548、CVE-2024-1553、CVE-2024-1547、CVE-2024-0751、  
CVE-2024-1549、CVE-2024-1550、CVE-2024-1552、CVE-2024-1546、CVE-2024-0749、CVE-2024-1551、



CVE-2024-0750、CVE-2024-0742、CVE-2024-0755、CVE-2024-0741、CVE-2024-24577、CVE-2023-22742、  
CVE-2023-49468 、 CVE-2023-49465 、 CVE-2023-27102 、 CVE-2023-49467 、 CVE-2023-27103 、  
CVE-2023-47471、CVE-2023-43887、CVE-2022-24720