高危漏洞排查

为加强信息系统（网站）安全，做好网络安全防护，请各单位开展以下风险排查，消除风险隐患，并加强网络安全监测。

一、Linux 内核存在权限提升高危漏洞

Linux 内核存在三个权限提升高危漏洞，可被攻击者利用获取主机最高 root 权限受影响产品包括Linux、部分使用 Linux 内核的 Linux 发行版，相关修复方案（详见附件 1、附件2）。

二、AI 编程工具 Claude Code 存在漏洞隐患

AI 编程工具Claude Code存在安全后门隐患，受影响的 Claude Code 版本为 2.1.91 至 2.1.196，完成国产AI替代编程。

三、部分信创产品存在安全漏洞

近期发现部分信创产品存在 12 个安全漏洞，其中高危 5 个、中危 5 个、低危 2 个，详见附件。根据相关厂商反馈，12 个漏洞均完成漏洞补丁修复。（详见附件 3）

附件：1、Linux 内核权限提升漏洞修复链接

2、麒麟、统信操作系统漏洞影响范围及修复措施

3、“通过安全可靠测评产品”漏洞汇聚共享清单

附件 1

Linux 内核权限提升漏洞修复链接

序号	漏洞名称	漏洞编号	受影响 Linux 内核版本	参考链接
1	Dirty Frag 漏洞	NVDB-C NVDB-20 26365718 /CVE-202 6-43284	4.11 系列 5.10 系列<5.10.255 5.15 系列<5.15.205 6.1 系列<6.1.171 6.6 系列<6.6.138 6.12 系列<6.12.87 6.18 系列<6.18.28 7.0 系列<7.0.5 7.1 系列<7.1-rc3	1) https://git.kernel.org/stable/c/a6cb440f274a22456ef3e86b457344f1678138f9 2) https://git.kernel.org/stable/c/ab8h995323e5237041472d07e5055f5f7dcdfl5b 3) https://git.kernel.org/stable/c/fe785bb3a8096dfcc4048a85cd0c83337eeecad 4) https://git.kernel.org/stable/c/5d55c7336f8032d434adcc5fa6987ccc93a44aec 5) https://git.kernel.org/stable/c/8253aab4659ca16116b522203c2a6b18dccacea7 6) https://git.kernel.org/stable/c/50ed1e7873100f77abad20fd3Ic51029bc49cd03 7) https://git.kernel.org/stable/c/b54edfle9a3fd3491bdcb82a21f8d21315271e0d 8) https://git.kernel.org/stable/c/7la1d9d985d26716f74d21118ee8cac821b06e97 9) https://git.kernel.org/stable/c/52646cbd00e765a6db9c3afe9535f26218276034 10) https://git.kernel.org/stable/c/f4c50a4034e62ab75fid5cdd191dd5f9c77fdff4 11) https://access.redhat.com/security/cve/cve-2026-43284 12) https://www.suse.com/security/cve/CVE-2026-43284.html 13) https://ubuntu.comsecurity/CVE-2026-43284 14) https://linux.oracle.com/cve/CVE-2026-43284.html 15) https://security-tracker.debian.org/tracker/CVE-2026-43284

序号	漏洞名称	漏洞编号	受影响 Linux 内核版本	参考链接
2		NVDB-CNVDB-2026923709/CVE-2026-43500	5.3 系列 6.6 系列<6.6.140 6.12 系列<6.12.88 6.18 系列<6.18.29 7.0 系列<7.0.6 7.1 系列<7.1-rc3	1) https://git.kernel.org/stable/c/7c504ffab3cfce8f7e4f463b314ae31030bdf18b 2) https://git.kernel.org/stable/c/3711382a77342a9a1c3d2e7330dcfc7ea927f568 3) https://git.kernel.org/stable/c/3eae0f40917206a4801efa5e0235c25bbdsa412c 4) https://git.kernel.org/stable/c/d45179f8795222cc858770dc619abc51f9d24411 5) https://git.kernel.org/stable/c/aa54b1d27fe0c2b78e664a34fd0fdf7cd1960d71 6) https://access.redhat.com/security/cve/cve-2026-43500 7) https://www.suse.com/security/cve/CVE-2026-43500.htm 8) https://ubuntu.com/security/CVE-2026-43500 9) https://linux.oracle.com/cve/CVE-2026-43500.html 10) https://security-tracker.debian.org/tracker/CVE-2026-43500

序号	漏洞名称	漏洞编号	受影响 Linux 内核版本	参考链接
3	Fradgnesia 漏洞	NVDB-CNVDB-2026284548/CVE-2026-46300	3.9 系列 5.10 系列<5.10.257 5.15 系列<5.15.208 6.1 系列<6.1.174 6.6 系列<6.6.141 6.12 系列<6.12.91 6.18 系列<6.18.33 7.0 系列<7.0.10 7.1 系列<7.1-rc5	1) https://git.kernel.org/stable/c/3599e6b3cclada96883d496a50a210d3afbb6987 2) https://git.kernel.org/stable/c/2f2b16022a2e10ca7bccfb98db5ed2ec0f72641c 3) https://git.kernel.org/stable/c/9d3e5fd19fe1063bf607219e8562tbd567b8e8d5 4) https://git.kernel.org/stable/c/78bf6b6bb19541d19tbda6242e7cfe2c682763c0 5) https://git.kernel.org/stable/c/760e1addc27bala7beb4a0a7e8b3e9ec49e7a34e 6) https://git.kernel.org/stable/c/3bd9e113d50034db99d7ef69fd8e5242d15e414a 7) https://git.kernel.org/stable/c/3884358a9286b17f389a72b1426fc4547c23c111 8) https://git.kernel.org/stable/e/f84eca5817390257cef78013d0112481c503b4a3 9) https://access.redhat.com/security/cve/cve-2026-46300 10) https://www.suse.com/security/cve/cVE-2026-46300.html 11) https:/ubuntu.com/security/CVE-2026-46300 12) https://linux.oracle.com/cve/CVE-2026-46300.html 13) https://security-tracker.debian.org/tacker/CVF-2026-46300

附件 2

麒麟、统信操作系统漏洞影响范围及修复措施

一、麒麟软件

（一）受影响产品型号

序号	产品名称	版本型号
1	银河麒麟桌面操作系统	VI0 SP1 2107
2		V10 SP1 2203
3		V10 SP1 2403
4		V10 SP1 2503
5		V11
6	银河麒麟高级服务器操作系统	V10
7		V10 SP1
8		V10 SP2
9		V10 SP3
10		V10 SP3 2403
11		V11

（二）补丁链接

https://support.kylinos.cn/#/security/cveDetail?allTitle=CVE-2026-43284

https://support.kylinos.cn/#/security/cveDetail?allTitle=CVE-2026-43500

https://support.kylinos.cn/#/security/cveDetail?allTitie=CVE-2026-46300

（三）临时缓解措施

1.实施说明

在部署正式补丁前，可采用以下临时缓解措施，无需重启

操作系统:

缓解措施 1: 禁用相关内核模块

$ sudo sh -c "printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' > /etc/modprobe.d/Fragnesia.conf; rmmod esp4 esp6 rxrpc 2>/dev/null; true"

回滚方式:更新内核补丁后可采用以下命令恢复配置。

$ sudo rm -f /etc/modprobe.d/Fragnesia.conf

$ sudo modprobe -a esp4 esp6 rxrpc 2>/dev/null

缓解措施 2: 禁止普通用户使用 unshare 系统调用创建 user namespace.

$ sudo sed -i '$a user.max_user_namespaces=0' /etc/sysctl.conf

$ sudo sysctl -p

回滚方式: 更新内核补丁后可采用以下命令恢复配置。

$ sudo sed -i '/^user.max_user_namespaces=0$/d' /etc/sysctl.conf

$ sudo sysctl -w user.max_user_namespaces='sysetl -a |grep "user.max_uts_namespaces"|awk'{print $3}' 1>/dev/null

补充:若操作系统被此漏洞利用可使用以下命令清理页缓存恢复。

$ echo 1 | sudo tee /proc/sys/vm/drop_caches

2.影响评估

禁用 esp4 esp6.rxrpc 模块后，依赖内核 ESP 协议和 AF_RXRPC 接口的 IPsec 加密通信及 AFS 文件系统将不可用。可能

影响基于内核的 IPsecVPN（如 StrongSwan、Libreswan 等），SD-WAN 组网或挂载 AFS 的服务，大多数应用(包括 OpenVPN、WireGuard 等非 IPsec VPN，以及 NFS/SMB 等常见网络文件系统)不依赖此模块，禁用后不受影响。

建议在生产环境执行前确认业务是否依赖内核 IPsec 隧道或 AFS 文件系统。

1) 缓解措施 1 会导致 esp4、esp6、rxrpc 模块功能无法使用，影响 IPsec/ESP 隧道(VPN)、Andrew File System(AFS)相关服务等

2) 缓解措施 2 会导致系统无法使用非特权进程建立用户命名空间，影响 rootless 容器、浏览器沙箱等,

二、统信软件

（一）受影响产品型号

序号	产品名称	版本型号
1	统信桌面操作系统专业版	V20
2	统信服务器操作系统	V20-D 版
3		V20-E 版
4		V20-C 版
5		V20-A 版

（二）补丁链接

https://src.uniontech.com/#/security_advisory?t=1780305448434，搜索漏洞编号 CVE-2026-43284、CVE-2026-43500、CVE-2026-46300 查询对应补丁。

（三）临时缓解措施

1.实施说明

1) 禁止后续加载模块

无论当前模块是否已加载，均建议在业务允许的情况下添加禁用配置，防止后续被自动或手动加载:

printf 'install esp4 /bin/false\ninstall esp6 /bin/false\ninstall rxrpc /bin/false\n' | sudo tee /etc/modprobe.d/disable-copy-fail-2.conf

2) 卸载已加载模块

如检测到相关模块已加载，可执行:

sudo rmmod esp4 esp6 rxrpc 2>/dev/null

如卸载失败，应检查是否存在业务进程占用、模块依赖。

3) 验证配置

grep -rE 'install (esp4|esp6|rxrpc) /bin/false' /etc/modprobe.d/disable-copy-fail-2.conf

返回以下内容即表示配置已写入:

install esp4 /bin/false

install esp6 /bin/false

install rxrpc /bin/false

配置完成后，服务器重启后相关模块也不会被再次加载，

4) 清理已被污染的 page cache

该类漏洞修改的是内存中的 page cache,不一定直接修改磁盘文件,若系统已经被测试或攻击，仅卸载和禁用模块不能清除已经被污染的 page cache; 后续执行 su 等目标程序时，仍可能命中被污染的内存页。建议在完成取证和业务评估后，优先通过重启清理内存状态。

确需在线清理时，请严格按照以下步骤执行:

#切换到 root 用户，清理所有 su

sudo su

killall su

#清理已被污染的 page cache

sudo sync

echo 3 | sudo tee /proc/sys/vm/drop_caches

5) 回滚方式

如确认业务受影响，需要恢复 csp4、esp6、rxrpc 模块加载能力，可删除禁用配置后按需加载模块:

sudo rm /etc/modprobe.d/disable-copy-fail-2.conf

sudo modprobe esp4

sudo modprobe esp6

sudo modprobe rxrpc

回滚前应确认系统处于受控环境，且已采取其他补偿性安全措施或已完成正式补丁升级。

2.注意事项

1) 缓解措施会禁用 esp4、csp6、rxrpc 模块，可能影响 IPsec ESP、部分 VPN/IPsec 业务、RxRPC/AFS 相关能力。生产环境操作前应完成业务影响评估，并优先在测试环境验证。

2) 华为线所有机型应按以下方式执行:

涉及华为线机型如下:pgv(w515、w585) pgw(w525) klu(L410) klv(L420、L540) pgx(w515x&w585x) flmx(L420x、L540x) pgy(w515y&w585y)

临时处置应采用以下方式:

修改/etc/default/grub.cfg，在 GRUB 内核启动参数 GRUB_CMDLINE LINUX DEFAULT=中加入以下内容:

initcall_blacklist=esp4_init,esp6_init,af_rxrpc_init

修改完成后执行以下命令更新 GRUB 配置并重启系统:

sudo update-grub

sudo reboot

重启后可通过以下命令确认启动参数已生效:

cat /proc/cmdline |grep 'initcall_blacklist=esp4_init,esp6_init,af_rxrpc_init'

该方式通过跳过 built-in 组件初始化降低攻击面，属于临时缓解措施，不等同于正式补丁。如启动异常，应通过 GRUB 引导菜单移除该启动参数后恢复。

回滚方式:

对于华为级机型，如已添加 initcall_blacklist=esp4_init,esp6_init,af_rxrpc_init 启动参数，回滚时应从/etc/default/gnub.cfg 中删除该内核启动参数，并执行以下命令更新 GRUB 置后重启系统:

sudo update-grub

sudo reboot

附件 3

“通过安全可靠测评产品”漏洞汇聚共享清单

产品信息			漏洞信息					消控处置信息		
序号	安可产品名称	厂商	漏洞编号	漏洞名称	漏洞分类	危害等级	汇聚单位	是否有补丁	是否发补丁	消控情况
1	方德桌面操作系统 V5.0（内核版本 5.4）	中科方德软件有限公司	CNNVD-2026-25392375	中科方德 NFSDesktop-5.0-G240-ord.polkit.cosappstore 中存在本地提权漏洞	代码问题	高危	CNNVD	是	是	已消控
2	统信桌面操作系统 V2.0（内核版本 5.10）	统信软件技术有限公司	CNNVD-2026-10084508	统信桌面操作系统本地权限提升漏洞	配置错误	高危	CNNVD	是	否	已消控
3	方德桌面操作系统 V5.0（内核版本 5.4）	中科方德软件有限公司	CNNVD-2026-79758741	中科方德 NFSDesktop-5.0-G240-timesync.service 中存在本地提权漏洞	配置错误	高危	CNNVD	是	是	已消控
4	方德桌面操作系统 V5.0（内核版本 5.4）	中科方德软件有限公司	CNNVD-2026-43696266	中科方德 NFSDesktop-5.0-G240-com.nfs.faillockd 中存在本地提权漏洞	配置错误	高危	CNNVD	是	是	已消控
5	方德桌面操作系统 V5.0（内核版本 5.4）	中科方德软件有限公司	CNNVD-2026-79074245	方德桌面操作系统存在本地提权漏洞	命令注入	高危	CNNVD	是	是	已消控
6	南大通用多模态数据库管理系统[简称: GBase 8c]V6	天津南大通用数据技术股份有限公司	CNNVD-2026-86698301	南大通用 GBase8c 数据库 SQL 注入漏洞	SQL 注入	中危	CNNVD	是	是	已消控
7	统信桌面操作系统 V2.0（内核版本 4.19）	统信软件技术有限公司	CNNVD-2026-10302592	UOS 桌面专业版 V20 1070 系统-com-deepin-daemon-Daemon 模块存在拒绝服务漏洞	其他	中危	CNNVD	是	是	已消控

产品信息			漏洞信息					消控处置信息		
序号	安可产品名称	厂商	漏洞编号	漏洞名称	漏洞分类	危害等级	汇聚单位	是否有补丁	是否发补丁	消控情况
8	万里安全数据库软件 V1.0	北京万里开源软件有限公司	CNNVD-2026-36103413	GreatDB CREATE SEQUENCE 功能存在缓冲区溢出漏洞	栈溢出	中危	CNNVD	是	是	已消控
9	万里安全数据库软件 V1.0	北京万里开源软件有限公司	CNNVD-2026-87020875	GreatSQL CREATE SYNONYM 功能存在缓冲区溢出漏洞	缓冲区溢出	中危	CNNVD	是	是	已消控
10	万里安全数据库软件 V1.0	北京万里开源软件有限公司	CNNVD-2026-60811609	万里数据库 GreatSQLgreatdb_ha 插件存在多处漏洞	未授权访问	中危	CNNVD	是	是	已消控
11	统信桌面操作系统 V2.0（内核版本 4.19）	统信软件技术有限公司	CNNVD-2026-49482069	UOS 桌面专业版 V20 1070 系统-com-deepin-daemon-REesourceManager 模块存在拒绝服务漏洞	其他	低危	CNNVD	是	是	已消控
12	统信桌面操作系统 V2.0（内核版本 4.19）	统信软件技术有限公司	CNNVD-2026-11440976	UOS 桌面专业版 V20 1070 系统-com-deepin-diskmanager 模块存在拒绝服务漏洞	其他	低危	CNNVD	是	是	已消控