麒麟操作系统漏洞检测实践指南

2025 年 12 月

前 言

随着国产化替代工作的深化，银河麒麟操作系统已成为政务、金融、能源、通信等关键领域的重要支撑，安全漏洞的检测直接关系到关键信息基础设施的安全防护成效。在行业实践中安全漏洞扫描产品对麒麟操作系统的误报问题日益突出。当前主流漏扫工具多依赖组件公开版本进行漏洞判定，导致本应排除的情况被误判为有效漏洞，进而引发用户、运维方与安全厂商的重复分析排查，大幅增加了安全管理的时间和人力成本。

为规范面向麒麟操作系统漏洞检测流程，提升漏洞扫描的准确性和效率，麒麟软件安全生态联盟邀请相关单位共同编写本指南。聚焦漏扫工具使用过程中的误报诱因，围绕“漏洞库更新状态”、“扫描方式选择”、误报标记过滤功能”、“白名单过滤机制”等，明确了误报产生的影响、判断依据和处理措施，为用户和运维方提供可操作的误报分析与处置策略。指导漏扫工具使用者科学配置、合理运用漏扫工具，精准识别麒麟操作系统的真实安全漏洞，有效规避误报。

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

北京升鑫网络科技有限公司

北京神州绿盟科技有限公司

深信服科技股份有限公司

北京猎鹰安全科技有限公司

哨云科技（南京）有限公司

漏洞误报分析处置典型策略

1、漏扫工具是否更新漏洞库

（1） 影响：如果在内网部署没有及时更新漏洞库，易产生误报。

（2） 判断依据：检查工具漏洞库更新时间和版本。

（3） 处理措施：用户侧运维人员手动更新漏洞库。

2、漏扫工具是否执行 ssh 登录/默认扫描

（1） 影响：如没有进行登录扫描，或执行默认扫描，会自动输出历年漏洞，易产生误报。

（2） 判断依据：工具使用手册对扫描方式的说明，以及是否需要获取操作系统版本号。

（3） 处理措施：用户侧联系安全厂商指导进行登录扫描。

3、漏扫工具是否提供扫描报告结论，以及提供解决方案或对策建议

（1） 影响：如扫描报告没有对漏洞处置进行说明或给出建议，易产生误报。

（2） 判断依据：漏扫报告是否对没有影响的漏洞给出忽略建议。

（3） 处理措施：通过与安全厂商对接，优化扫描报告输出模板。

4、漏扫工具是否提供误报标记过滤扫描结果

（1）影响：如无标记功能，易产生误报。

（2）判断依据：产品使用手册或标记功能介绍。

（3）处理措施：在漏扫工具的相应功能设置标记误报，优化扫描输出。

5、漏扫工具是否根据白名单（对麒麟操作系统无影响的漏洞）过滤扫描结果

（1） 影响：如没有对无影响漏洞进行过滤，易产生误报。

（2） 判断依据：是否使用白名单对无影响的漏洞进行过滤。

（3） 处理措施：通过与安全厂商对接，使用白名单过滤，优化扫描输出。

麒麟操作系统漏洞检测实践（奇安信）

1、用户判断分析处置

漏扫工具是否更新漏洞库：系统自动更新漏洞库。

漏洞编号	漏洞名称	漏洞等级	威胁类型	来源	影响范围	公开日期
CVE-2025-10235 | QVD-2025-35...	Scada-LTS代码执行漏洞(CVE-2025-10235)	低危	代码注入	cve	低	2025-09-11
CVE-2025-10234 | QVD-2025-35...	Scada-LTS代码执行漏洞(CVE-2025-10234)	低危	代码注入	cve	万级	2025-09-11
CVE-2025-6088 | QVD-2025-35183	danny-avila librechat权限提升漏洞(CVE-2025-6088)	中危	权限提升	cve	低	2025-09-11
CVE-2025-8388 | QVD-2025-35085	WordPress PowerPack Elementor Addons代码执行漏洞(CVE-2025-...	中危	代码注入	cve	万级	2025-09-10
CVE-2025-9622 | QVD-2025-35090	WordPress WP Blast代码执行漏洞(CVE-2025-9622)	中危	信息泄漏，代码注入	cve	万级	2025-09-10
CVE-2025-9888 | QVD-2025-35088	Maspik代码执行漏洞(CVE-2025-9888)	中危	信息泄漏，代码注入	cve	万级	2025-09-10
CVE-2025-10197 | QVD-2025-34...	HJSoft HCM SQL注入漏洞 (CVE-2025-10197)	中危	代码注入，信息泄...	cve	低	2025-09-10
CVE-2025-9463 | QVD-2025-35091	WordPress WooCommerce代码执行漏洞(CVE-2025-9463)	中危	信息泄漏，代码注入	cve	万级	2025-09-10
CVE-2025-56578 | QVD-2025-35...	RTSPtoWeb 任意代码执行漏洞 (CVE-2025-56578)	待定级	身份验证绕过	cve	万级	2025-09-10
CVE-2025-56466 | QVD-2025-35...	Dietly硬编码凭据漏洞 (CVE-2025-56466)	待定级	信息泄漏	cve	万级	2025-09-10

图 1：漏洞更新信息

2、处置措施和操作步骤

检查漏洞库版本：用户侧运维人员与安全厂商进行对接，判断当前漏洞库版本是否滞后。

同步最新漏洞库：安全厂商与用户侧运维人员进行对接，在用户侧部署同步最新的漏洞库。

3、用户侧判断漏洞存在情况

（1）操作系统类型判断：用户根据组件报告以及样本文件头，判断操作系统类型

（2）发行版及架构判断：用户通过多种方式判断操作系统具体的发行版以及指令集架构，以麒麟操作系统软件 ffmpeg 为例。

在编译标签中搜索二进制的操作系统信息：

strings ffmpeg | grep -i "arm"

-> --prefix=/usr --extra-version=1kylin1k23.10 --toolchain=hardened --libdir=/usr/lib/aarch64-linux-gnu --incdir=/usr/include/aarch64-linux-gnu --arch=arm64 --enable-gpl --disable-stripping --enable-avresample --disable-filter=resample

--enable-avisynth --enable-gnutls --enable-ladspa --enable-libaom --enable-libass
--enable-libbluray --enable-libbs2b --enable-libcaca --enable-libcdio --enable-libcodec2
--enable-libflite --enable-libfontconfig --enable-libfreetype --enable-libfribidi
--enable-libgme --enable-libgsm --enable-libjack --enable-libmp3lame --enable-libmysofa
--enable-libopenjpeg --enable-libopenmpt --enable-libopus --enable-libpulse
--enable-librsvg --enable-librubberband --enable-libshine --enable-libsnappy
--enable-libsoxr --enable-libspeex --enable-libssh --enable-libtheora --enable-libtwolame
--enable-libvidstab --enable-libvorbis --enable-libvpx --enable-libwavpack --enable-libwebp
--enable-libx265 --enable-libxml2 --enable-libxvid --enable-libzmq --enable-libzvbi
--enable-lv2 --enable-omx --enable-openal --enable-opencl --enable-opengl --enable-sdl2
--enable-libdc1394 --enable-libdrm --enable-libiec61883 --enable-chromaprint
--enable-frei0r --enable-libx264 --enable-shared

可从 string 信息中读取到 kylin1k23.10 和 arm64 等关键信息。

漏洞存在判断：用户根据样本的操作系统以及漏洞官方公告判断是否存在。

（3）用户侧判断漏洞函数调用

提取漏洞函数信息：用户从 CVE 描述或安全公告中获取漏洞函数信息。

调用链跟踪：用户通过 strace、ltrace 等工具追踪调用行为。

动态调试：用户通过调试工具观察漏洞函数内存状态并验证调用链。

函数调用判断：用户根据动态追踪以及官方公告信息判断当前漏洞是否被调用。

（4）用户侧判断漏洞环境条件

环境条件收集：用户根据样本的来源，确认漏洞组件的环境条件，如

发行版及版本（lsb_release -a）、内核版本（uname -r）、架构类型（uname -m）

服务运行状态（systemctl status $server）、SE 状态（getenforce）、当前动态链接库（ldd $binary）、SUID/SGID 文件（find / -perm -4000 -o -perm -2000 -type f）

用户权限（id、groups）、网络可达性（ping、nc）、防火墙（iptables、firewall-cmd）

内核保护机制（SMEP/SMAP、KASLR）、环境变量（printenv）等

漏洞可利用判断：用户根据漏洞官方公告以及当前运行环境确定漏洞是否可利用。

（5）白名单验证与处置

验证白名单功能：用户侧运维人员与安全厂商进行对接，根据测试结果判断白名单是否开启。

同步最新漏洞库：安全厂商与用户侧运维人员进行对接，在用户侧维护漏洞白名单。

（6）漏洞打标记 正确 OR 误报

组件名称	版本号	组件类别	组件相似度	漏洞分布	状态	操作
openjpeg	2.3.0	native	96.42	严重(3) 高危(10) 中危(13) 低危(0) 待定级(0)	待确认	确认
ffmpeg	3.4.1	native	74.41	严重(2) 高危(10) 中危(16) 低危(0) 待定级(0)	待确认	确认
ffmpeg	3.4.1	native	95.28	严重(2) 高危(10) 中危(16) 低危(0) 待定级(0)	待确认	确认
libvpx	1.6.1	native	66.19	严重(1) 高危(2) 中危(1) 低危(0) 待定级(0)	待确认	确认
libvorbis	1.3.5	native	97.53	严重(1) 高危(1) 中危(3) 低危(0) 待定级(0)	待确认	确认
libass	0.14.0	native	52.10	严重(0) 高危(2) 中危(0) 低危(0) 待定级(0)	待确认	确认
bzip2	1.0.6	native	96.43	严重(0) 高危(1) 中危(1) 低危(0) 待定级(0)	待确认	确认
fribidi	0.19.7	native	58.49	严重(0) 高危(0) 中危(2) 低危(1) 待定级(0)	待确认	确认
lame	3.99	native	96.67	严重(0) 高危(0) 中危(2) 低危(0) 待定级(0)	待确认	确认
Accord.Imaging	2.5.3.0	dotnet	52.08	严重(0) 高危(0) 中危(0) 低危(0) 待定级(0)	待确认	确认

图 2：打开报告详情

点击分析结果确认，正确或错误进行标记

图 3：分析结果确认

（7）完成漏洞修改的验证方法

点击项目重新分析按钮，进行分析，查看重新分析结果是否还包含之前漏洞。

图 4：漏洞验证

（8）用户判断信息

表：用户判断信息模板

字段	填写说明
操作系统版本	麒麟具体版本（如 Kylin V10 SP1）
部署套数	受影响的系统部署数量
实施扫描时间	漏洞扫描的具体时间
部署位置	系统部署环境（内网隔离区/外网云服务器/混合云）
用户名称	受影响单位或部门名称
集成/运维操作方	用户侧维护人员
安全厂商名称	奇安信
漏扫工具名称	天问平台
扫描报告附件	漏洞扫描报告（PDF/JSON 格式）
其他问题需求	更新漏洞库等需求

麒麟操作系统漏洞检测实践（安恒）

明鉴漏洞扫描系统（明鉴漏扫）是一款融合安恒多年信息安全漏洞挖掘、渗透测试技术研究和漏洞检查方法的最佳实践经验，集主机安全扫描、网站安全扫描、数据安全扫描、弱口令发现和基线配置核查于一身的产品，能够精准评估多维度资产的安全风险，帮助用户提高网络安全防护性能和抗破坏能力。

1、检查任务下发

说明：由于漏洞检测的原理，在扫描前需保证扫描器与目标之间网络可达。因此，扫描前需要确认漏扫到目标机中间是否有安全防护（防火墙/EDR/上网行为管理等各种安全设备或策略），若存在安全防护，请及时将漏扫 IP 加白，否则会导致无法检出漏洞或漏洞结果不准确等情况。在此基础之上，请参考下述说明进行配置即可。

明鉴漏扫不仅可以对国内外操作系统下发漏洞扫描任务，也可以单独对国产信创环境下发单独“信创漏洞扫描任务”，麒麟系统可按照该任务执行，检测更有针对性。

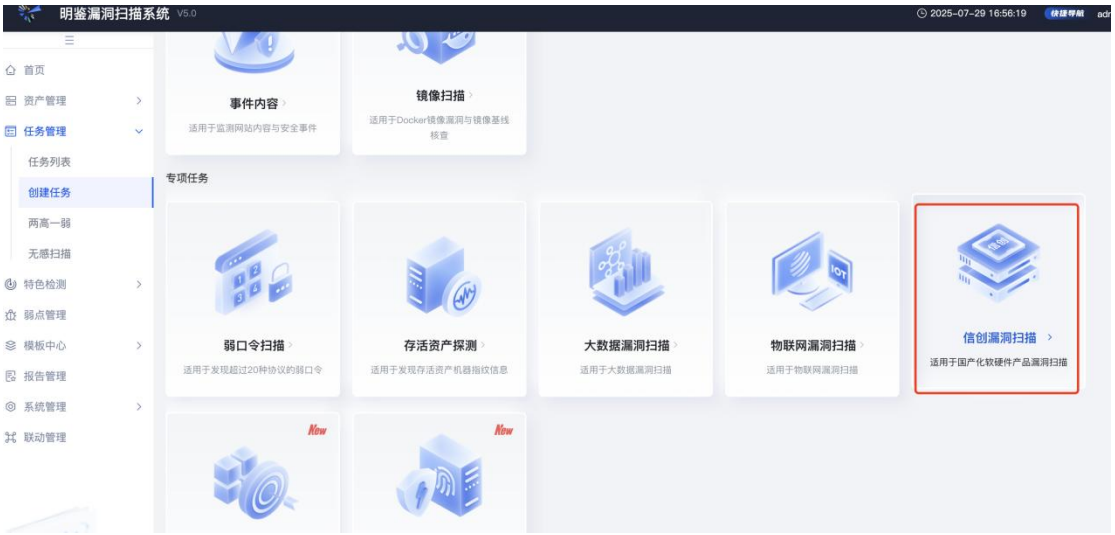


图 1：系统信息

2、任务参数配置

麒麟系统扫描最佳配置建议从策略模板、端口列表。两个维度来进行修改配置，其余参数使用默认配置即可，详情如下：

下发主机扫描时。策略模板建议选择“全部漏洞扫描”如下图所示：

图 2：任务参数配置

随后点击下一步，在高级参数栏中，存活探测方式修改为“适中”，端口列表为“所有 TCP”，如下图所示：

图 3：新建主机

麒麟系统扫描建议通过登录授权方式进行漏洞扫描，检测准确性更高

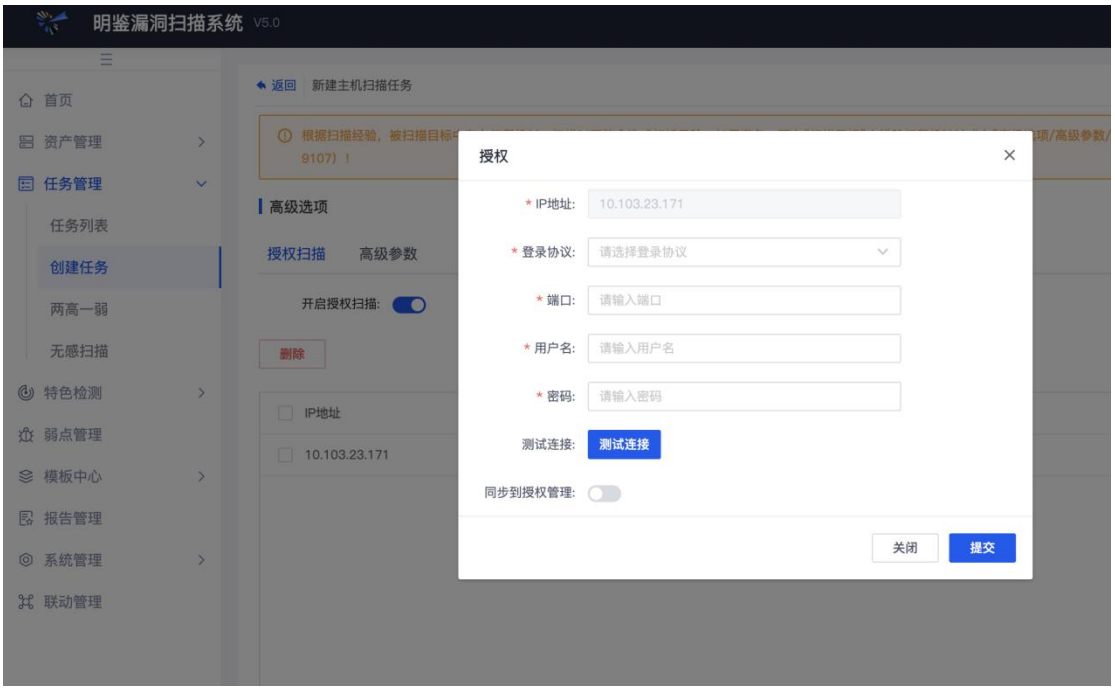


图 4：主机扫描任务

3、任务信息查看

明鉴漏扫任务执行结束支持在线预览扫描结果，包括任务信息概览、漏洞分布、开放端口、完整在线报告等。

图 5：任务信息

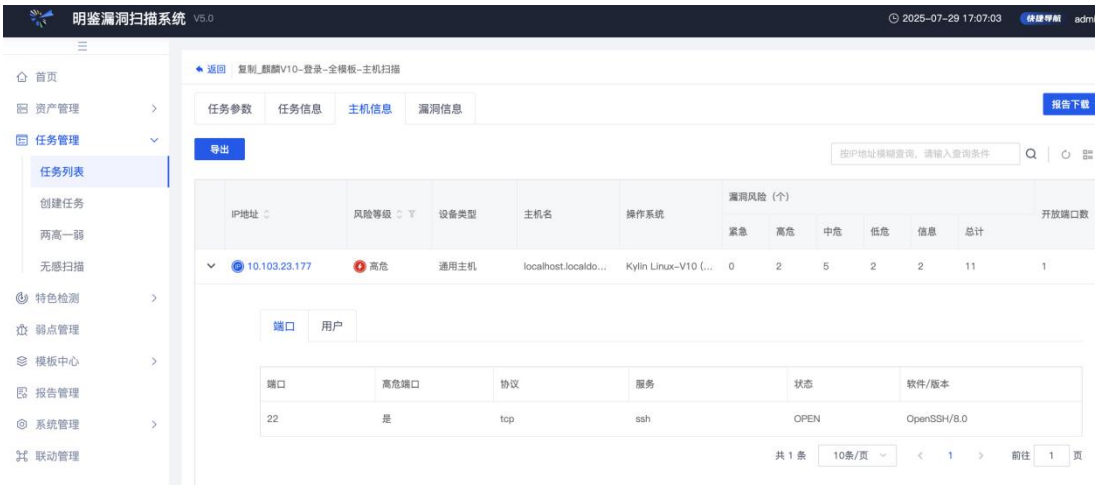


图 6：任务列表

4、漏洞信息查看

所有漏洞信息可以在线查看详情信息，可在线掌握漏洞风险等级、漏洞 poc、EXP 等标签和修复建议等。

图 7：漏洞详情

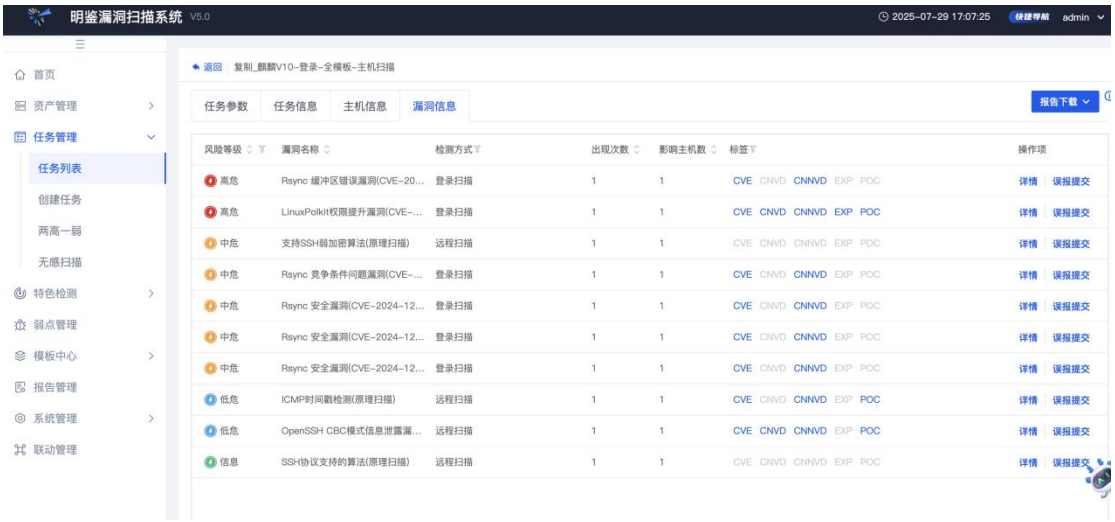


图 8：漏洞信息

5、漏洞分析

策略返回信息查看。可以在漏洞详情中查看策略反馈信息，分析被测目标服务信息。

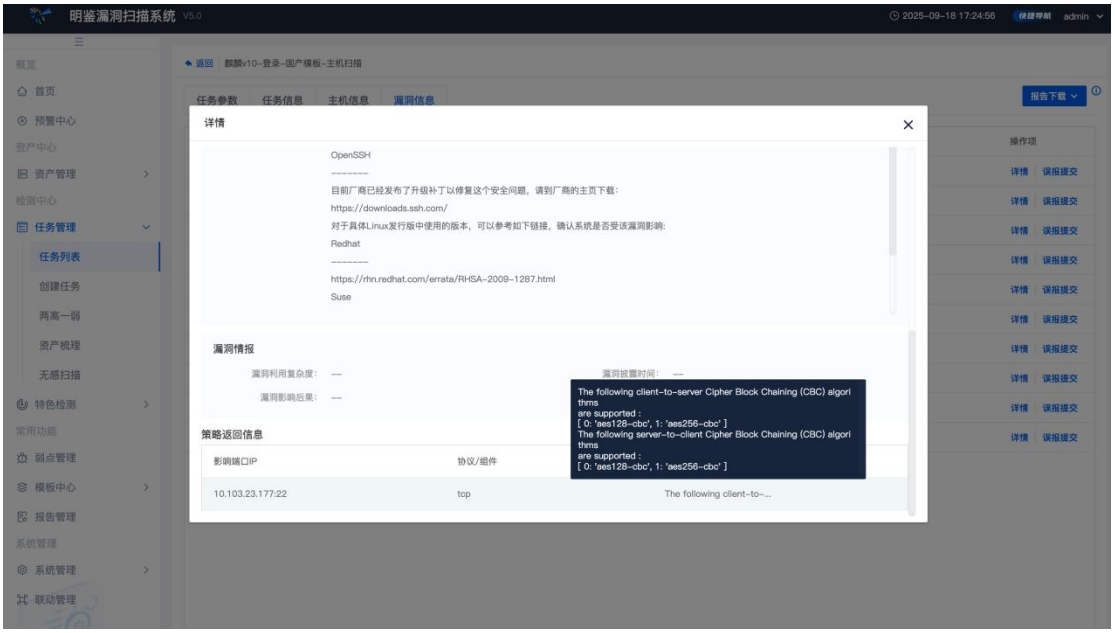


图 9：漏洞详情

6、漏洞 EXP 取证

针对存在 EXP 的漏洞，可直接在产品界面进行渗透取证（保障业务安全前提下进行）。

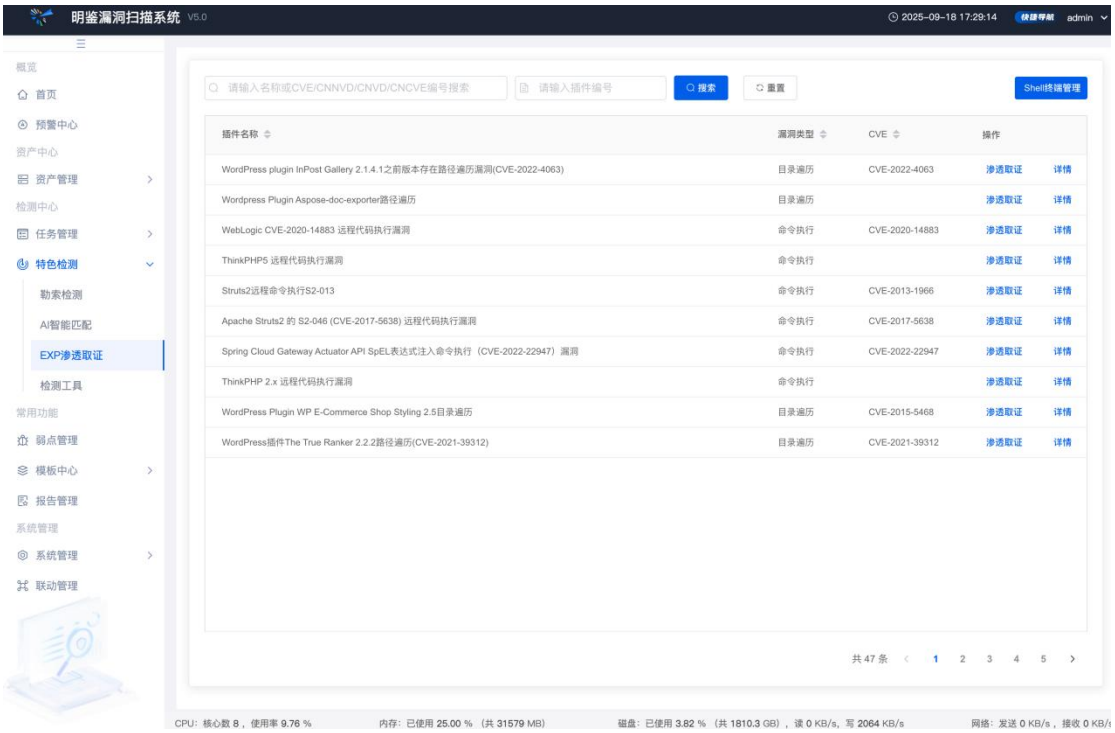


图 10：取证信息

7、漏洞误报处理

经判断，检查出漏洞实际不存在，是漏扫误报情况下可直接在任务结果中点击误报处理。

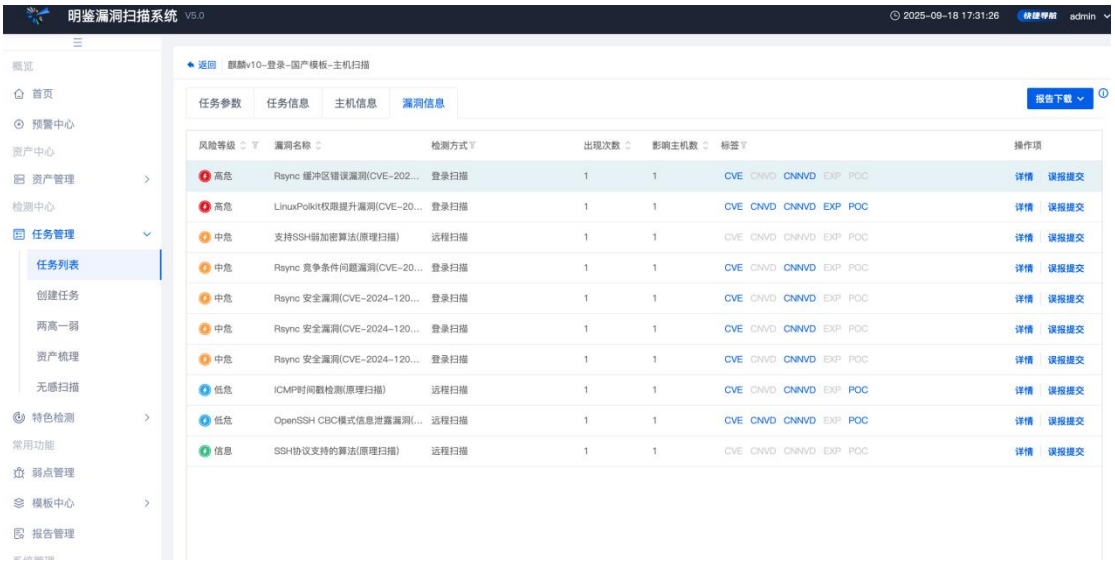


图 11：误报处理

对已确定某策略误报高，经评估不需要检测时，可以在自定义策略中排除该策略，后续任务不再调该插件，避免持续误报。

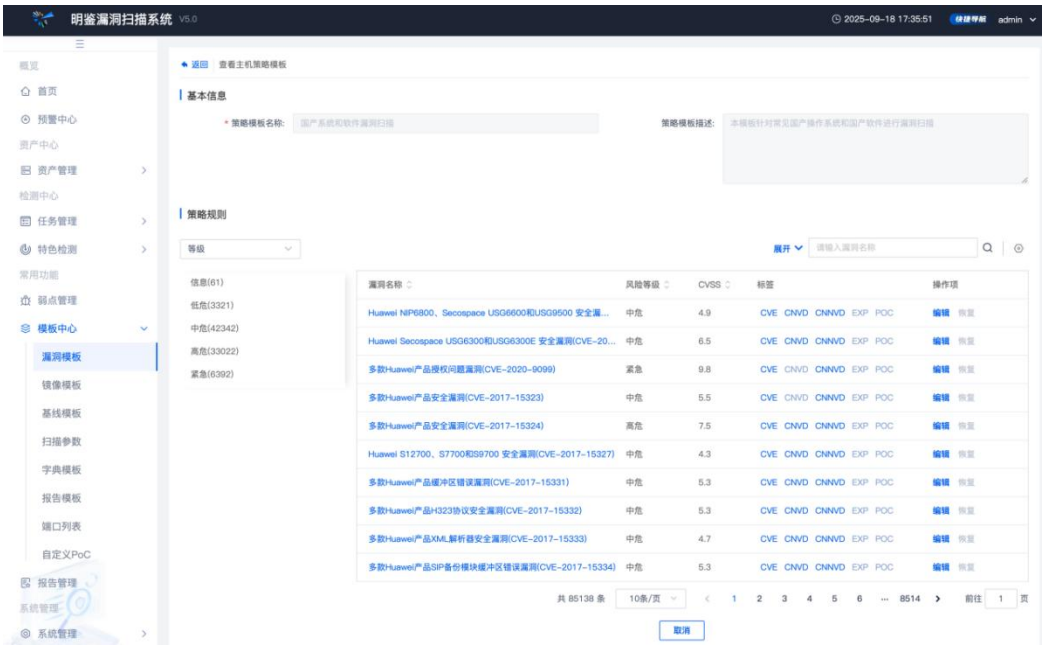


图 12：策略规则

8、离线报告输出

通过产品报告管理模块可以基于任务、单资产维度输出详细风险评估报告。报告格式支持 word、Excel、pdf、HTML、XML，报告模板可根据场景需要做高度自定义，输出更聚焦的脆弱点评估报告。

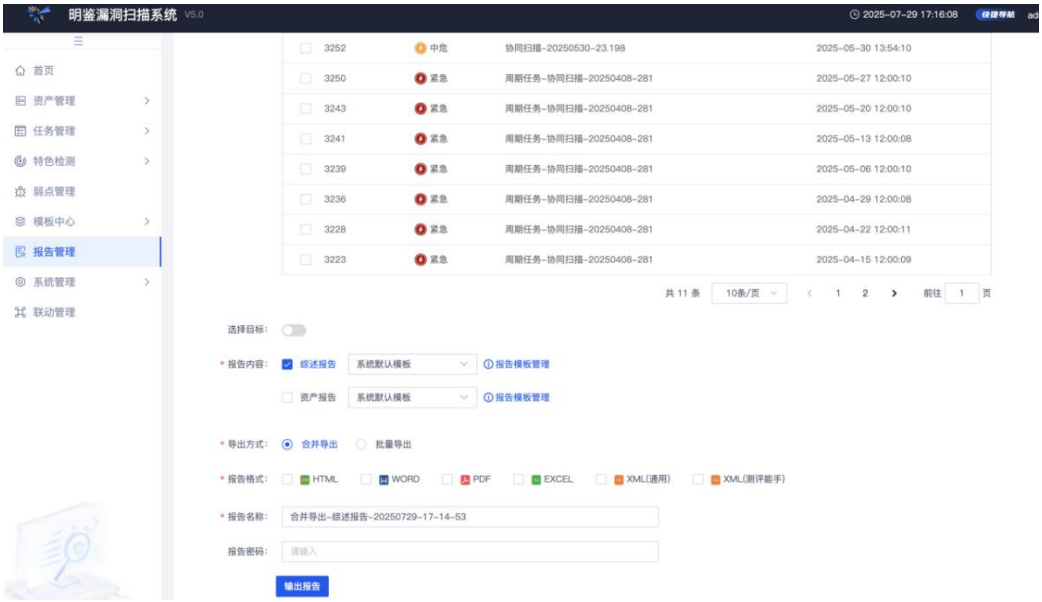


图 13：漏洞报告

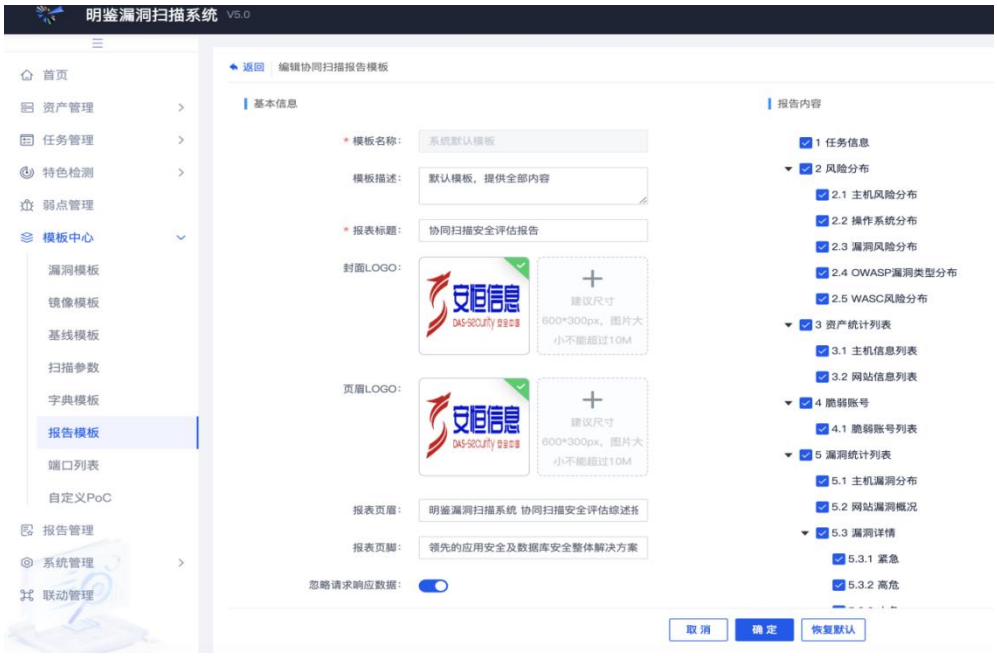


图 14：扫描报告

9、其他

检查设备系统版本是否最新，如下图所示，点击“系统管理”，“系统设置”检查设备系统版本和策略版本是否最新。

图 15：系统升级

检查设备策略版本是否最新，如上图所示，点击“立即升级”若无可更新升级包，则设备所有组件均为最新。主机策略、web 策略均为一周一更新。若策略版本不是最新，可能会导致扫描结果误报。

麒麟操作系统漏洞检测实践（天融信）

1、漏洞扫描前更新漏洞库

漏洞库同步：天融信漏扫内置“国产化漏洞”模板，漏洞库信息与麒麟官方安全公告保持同步，确保麒麟操作系统特有的漏洞及时更新，漏洞扫描前需要更新漏洞库。

漏洞库可以通过离线升级或者在线升级的方式更新。

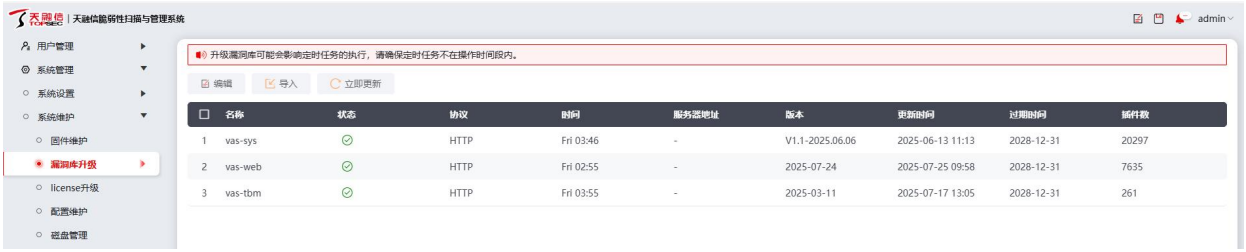


图 1：漏洞库升级功能

漏洞库离线升级操作步骤：

在“漏洞库升级”页面，“导入”漏洞库升级包即可。

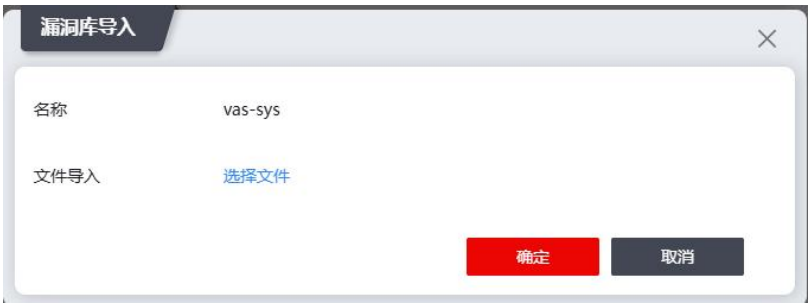


图 2：漏洞库离线导入

漏洞库在线升级操作步骤：

在“漏洞库升级”页面，“编辑”漏洞库定期升级策略，能够定期自动升级；选择“立即更新”能够将设备和漏洞库服务器上的版本进行对比并自动最新漏洞库。

图 3：自定义漏洞库更新方式

升级成功后漏洞库版本会同步更新。

2、扫描策略：配置 SSH 登录扫描

登录认证配置：使用 SSH 协议登录，天融信漏扫支持登录凭证检测功能，确保登录认证。

操作步骤：在系统扫描任务“高级配置”中选择“登录扫描配置”，添加“ssh 协议”，输入靶机的账号和密码，点击登录检测，验证账号密码是否登录成功，账号验证成功后再进行扫描。

图 4：未配置登录扫描

图 5：未配置登录扫描扫到的漏洞

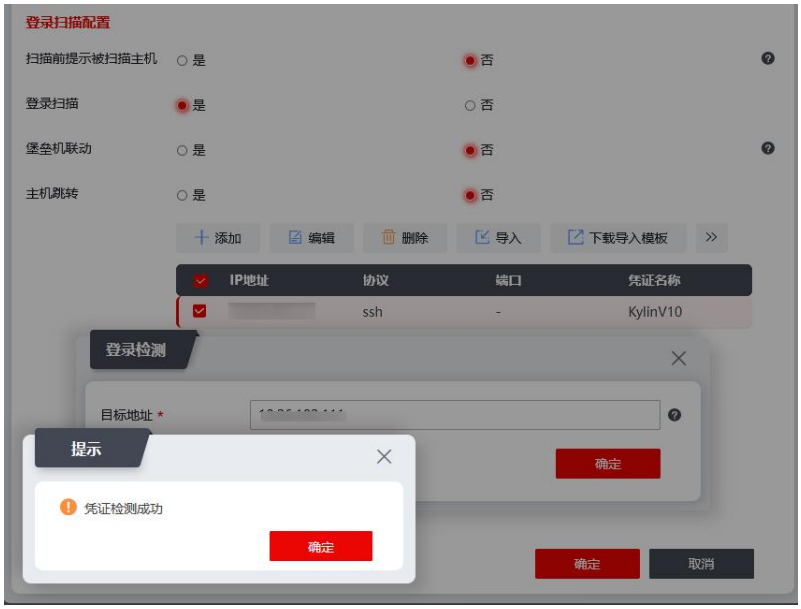


图 6：配置登录扫描，并校验登录凭证

图 7：配置登录扫描扫到的漏洞

3、扫描报告结论及解决方案

扫描任务结束后，天融信漏扫提供了在线报表和离线报表，报表中对漏洞处置进行说明及解决方案，用户可以通过报表中提供的解决办法来修复漏洞；

操作步骤：扫描完成后，点击报告中的麒麟漏洞查看处置说明和解决方案，依据方案安装补丁，修复漏洞。

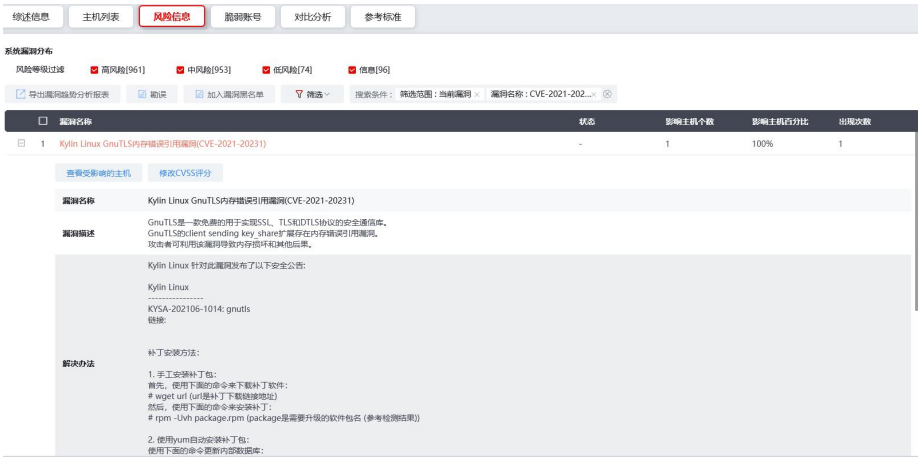


图 8：查看在线报表中漏洞的解决办法

图 9：生成离线报表

图 10：查看离线报表中漏洞的解决办法

4、提供误报标记过滤功能

天融信漏扫支持通过“勘误”对上报的漏洞进行标记过滤。

操作步骤：进入在线报表“风险信息”页面，对漏洞进行勘误，勘误功能支持隐藏或删除漏洞，勘误后的漏洞不会出现在导出的离线报告中，隐藏的漏洞再次筛选并恢复。

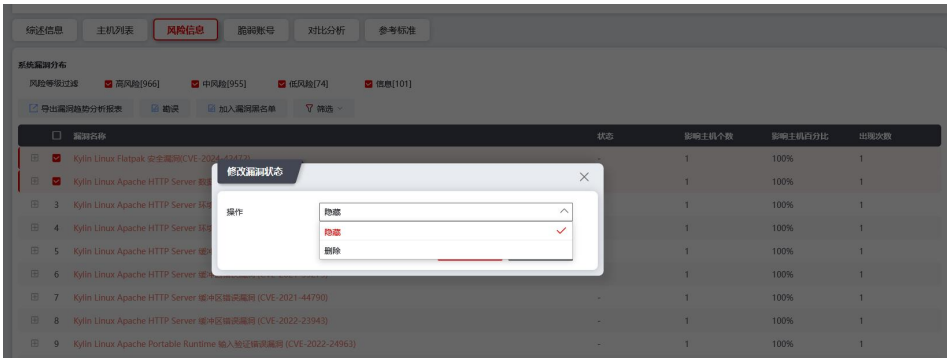


图 11：在线报表中对漏洞进行勘误

勘误漏洞：勾选漏洞名称后点击“勘误”按钮选择勘误状态，“确定”提交即可。

图 12：勾选单条漏洞

批量勘误漏洞：需要同时勾选多条需要被勘误的漏洞名称。

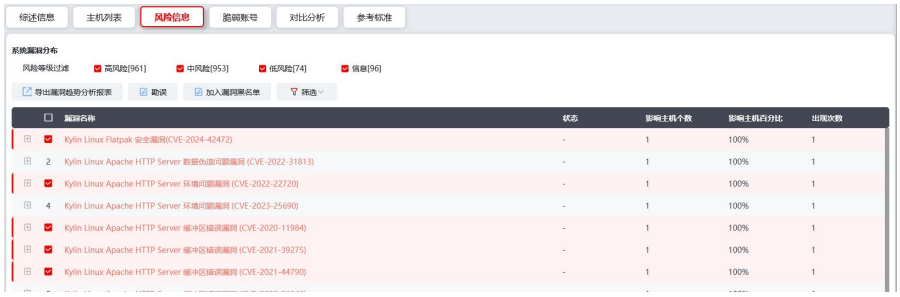


图 13：勾选多条漏洞

图 14：查看已勘误（隐藏）的漏洞

图 15：勘误前生成的离线报告包含所有漏洞信息

图 16：勘误后生成的离线报告不包含已勘误的漏洞信息

5、根据白名单过滤扫描结果

天融信漏扫支持通过“漏洞黑名单”和自定义模板两种方式过滤扫描结果。

漏洞黑名单操作步骤：（1）在在线报表页面将误报的漏洞加入“漏洞黑名单”，后续不会再上报漏洞黑名单列表中的漏洞。（2）进入系统漏洞黑名单菜单，添加需要过滤的漏洞。

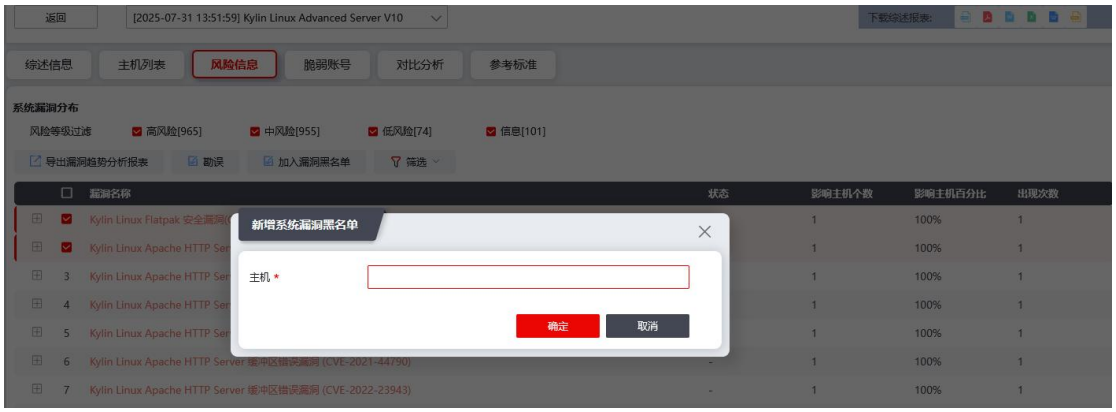


图 17：在线报表中新增漏洞黑名单

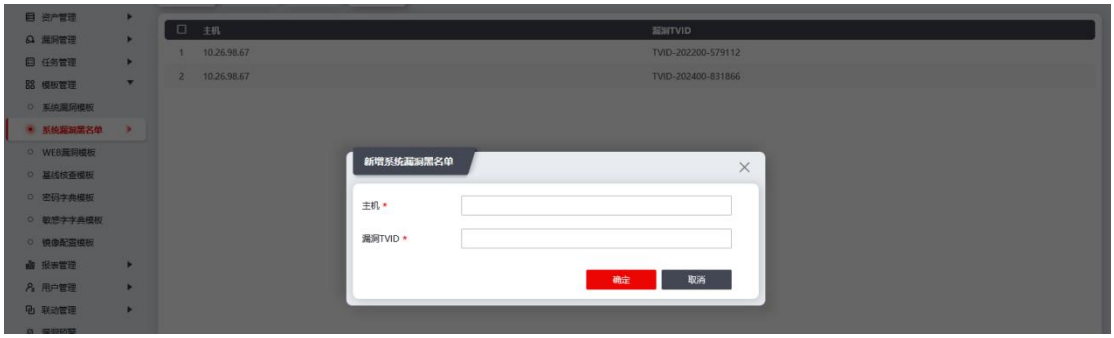


图 18：系统漏洞黑名单中新增漏洞黑名单

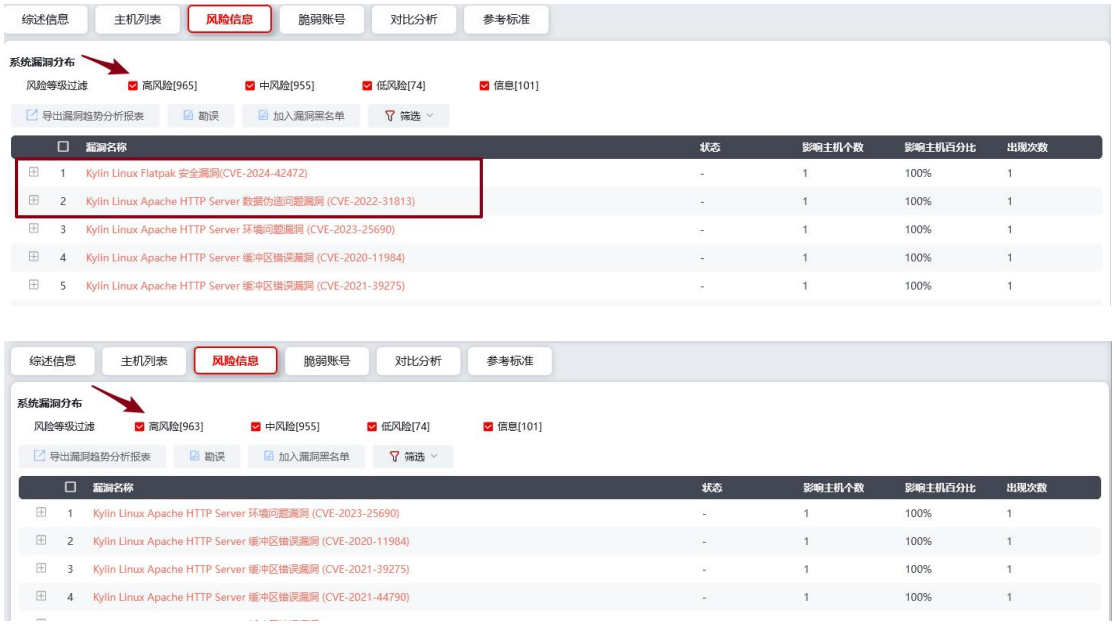


图 19：加入系统漏洞黑名单的漏洞被过滤

自定义模板操作步骤：进入模板管理，系统漏洞模板页面，使用添加模板功能，筛选出需要检测的漏洞并创建模板，在下发任务时选择自定义的的模板，同样可以过滤扫描结果。

图 20：自定义一个 CVE-2024 的系统漏洞模板

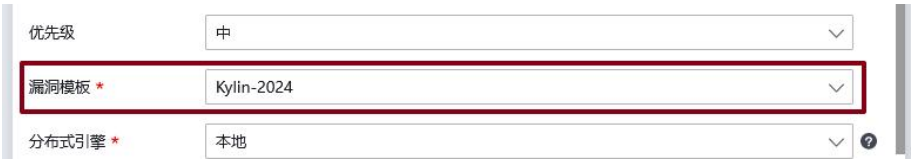


图 21：下发系统扫描任务选择自定义的系统漏洞模板

不在自定义漏洞模板的漏洞没有上报：

图 22：自定义模板扫描结果

麒麟操作系统漏洞检测实践（中科微澜）

1、扫描方式

在微瞳漏洞扫描系统平台【资产管理】的【添加资产】里添加系统为KylinLinuxAdvancedServerV10 的主机，选择 SSH 的连接方式，输入要检测的目标主机的 IP 地址，用户名和密码，勾选下面的“启用 Agent 推送”，将 Agent 安装程序推送到目标服务器，并将 Agent 安装在服务器上，然后点击保存任务，然后可以在资产管理中主机下面的列表页看到该主机的部分资产信息，点击该资产右边的立即检测图标，开始对该主机进行检测。

除了上述的 SSH 连接外，还可以通过 telnet 进行连接，平台还支持多种 Agent 分发方式，可以选择手动安装或是一键推送，例如加入资产管理计划后，无需在目标设备上执行安装操作，就可以实现 Agent 一键自动推送。平台会定时检查登录配置信息的准确性，确保目标主机的连接处于正常状态。

图 1：添加资产操作

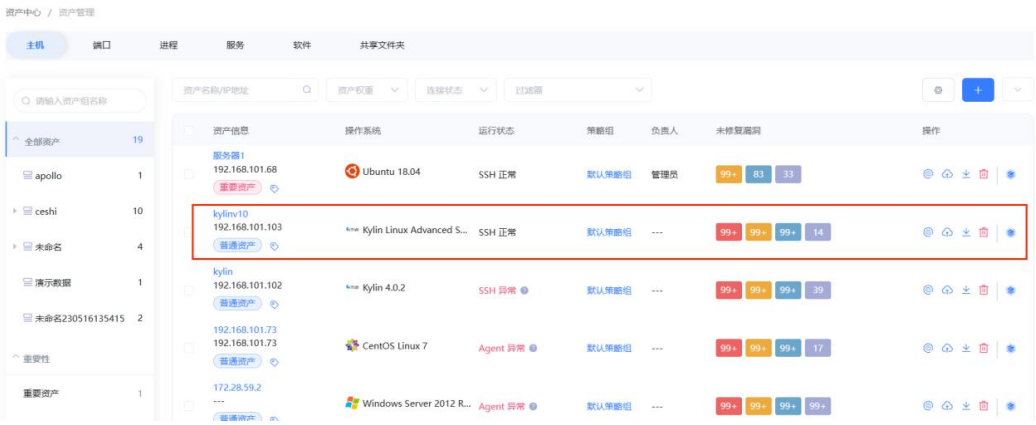


图 2：主机运行状态检验

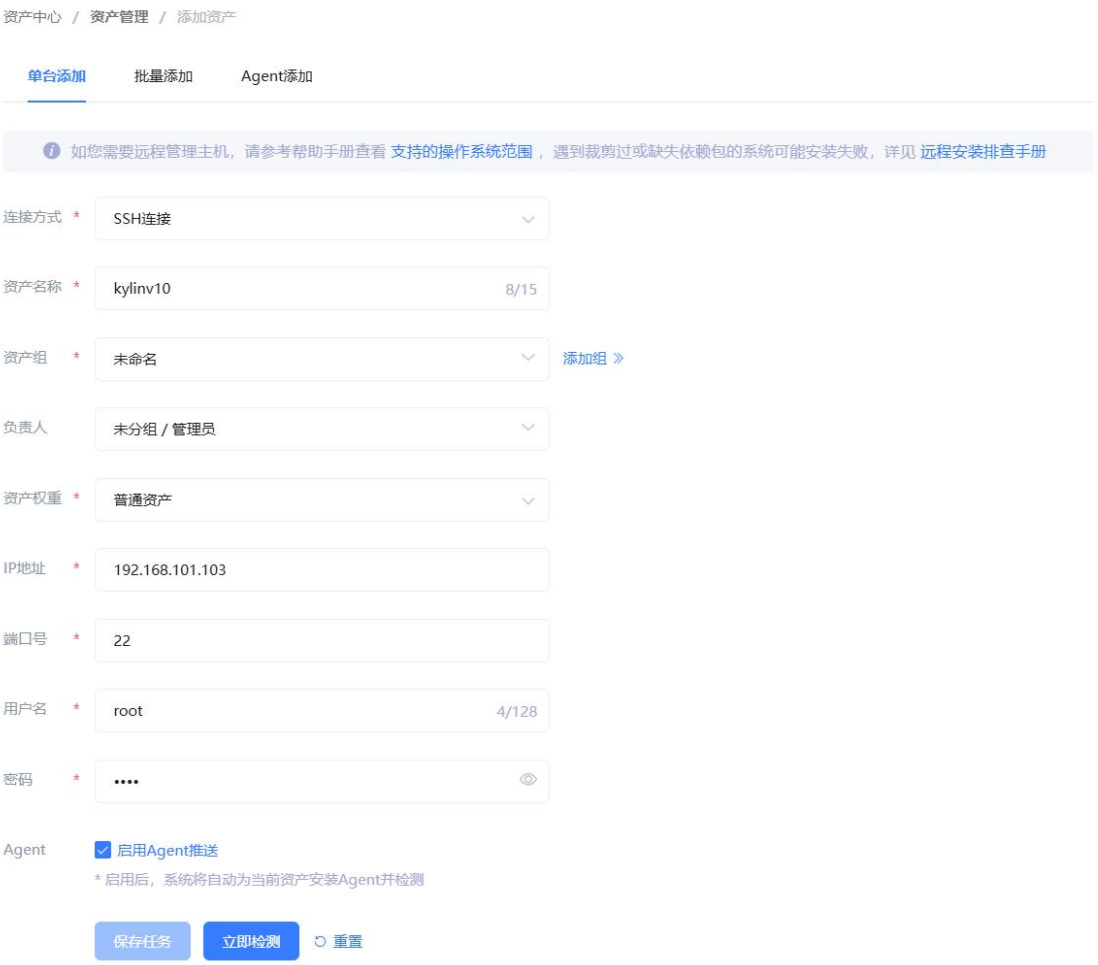


图 3：三种连接方式：ssh、telnet、agent 一键推送

2、资产信息查看

资产信息检测完成后，可对检测结果进行查看。点击资产名称，进入到资产信息界面，在基本信息页面可以看到该资产的操作系统是 KylinLinuxAdvancedServerV10，对应内核版本为 4.19.90-52.22.v2207.ky10.x86_64，IP 地址为 192.168.101.103，漏洞数量 1183，主机风险状态比较严重，除此外还可以看到连接方式、连接状态、网络连接等信息，使相关安全人员对主机资产信息有较为清晰的认知。

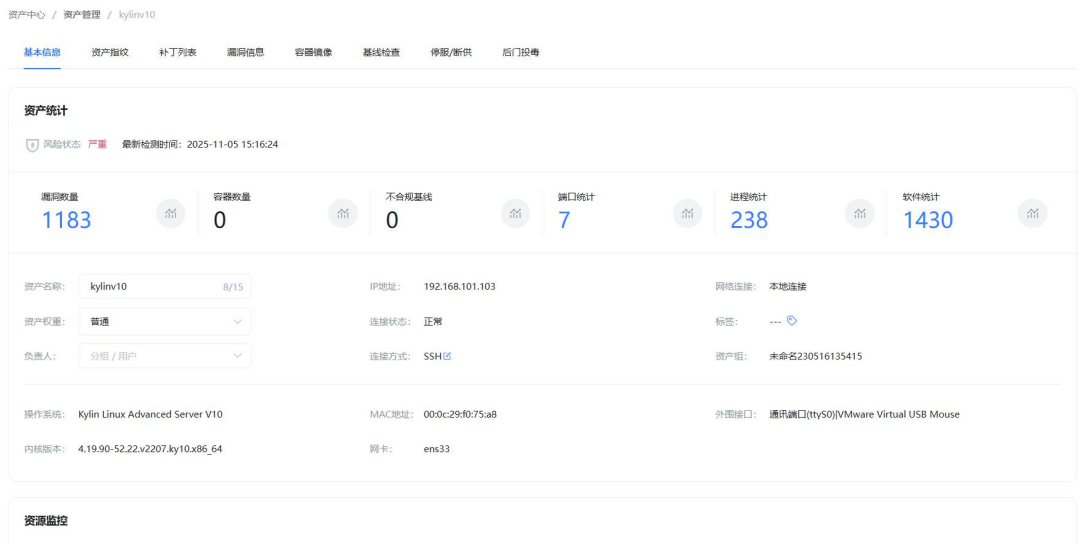


图 4：资产信息页面

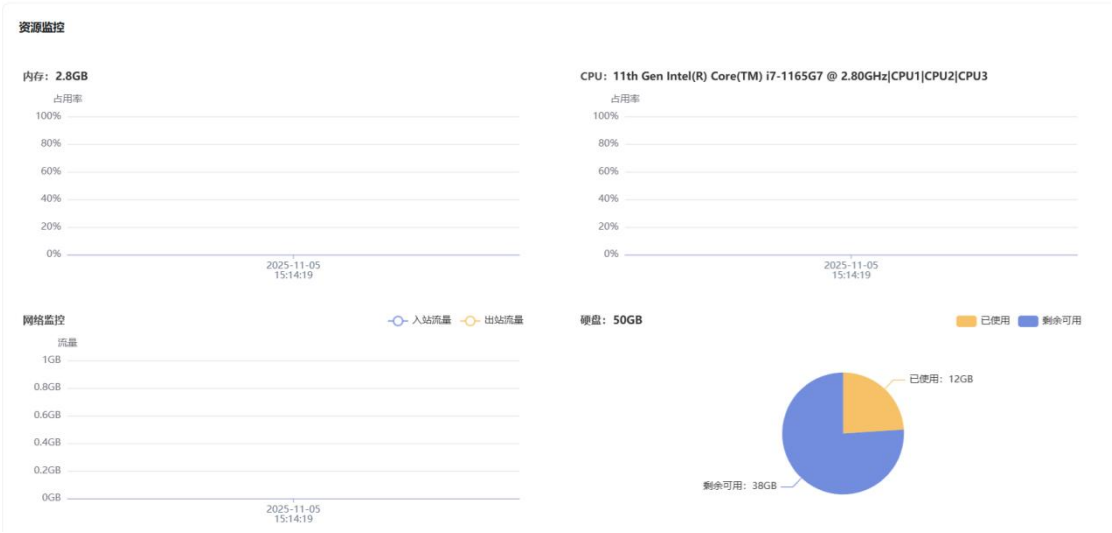


图 5：资产信息资源监控

3、漏洞结果查看

列表页漏洞信息： 查看 KylinLinuxAdvancedServerV10 系统的漏洞情况，如漏洞的名称、漏洞标签、受影响的软件包、修复优先级、漏洞编号、检测时间、修复状态等信息。通过“漏洞名称/编号”筛选框能够快速定位漏洞，通过“软件包”下拉框可以看到所有受影响的软件包名称，帮助安全人员查询对应软件包的漏洞信息。

漏洞的修复优先级将需要修复的漏洞分为四个等级：需立即修复、需尽快修复、可延后修复、暂可不修复。除此外还可以看到每个漏洞对应的优先级得分以及每个计算因子的分值（资产权重因子、CVSS 评分、环境因子、威胁因子、PoC），

优先级得分越高对应的修复优先级就越高。安全人员可以针对漏洞的修复等级以及修复优先级得分准确、快速定位急需修复的关键漏洞。

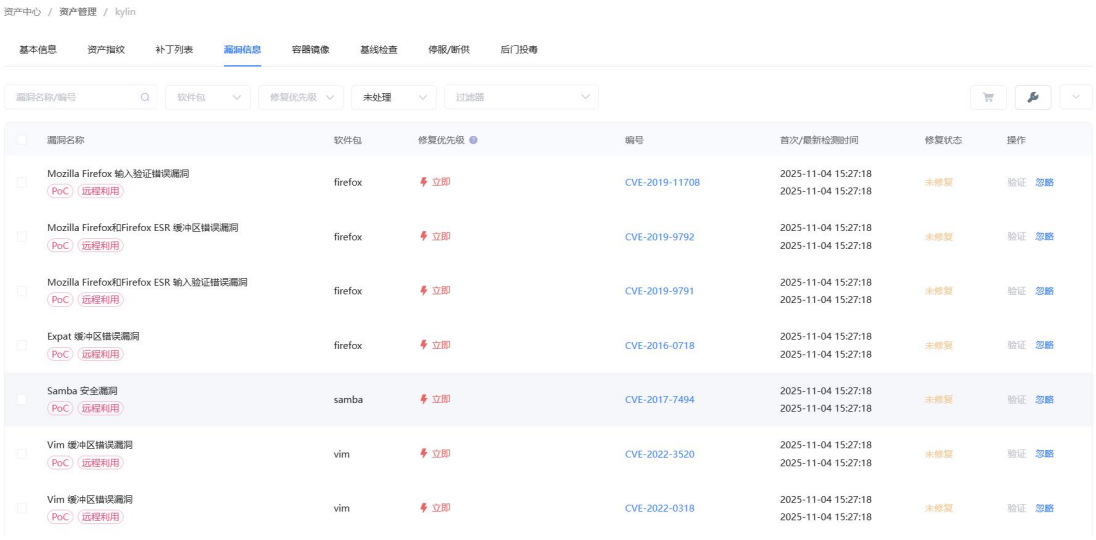


图 6：列表页漏洞信息

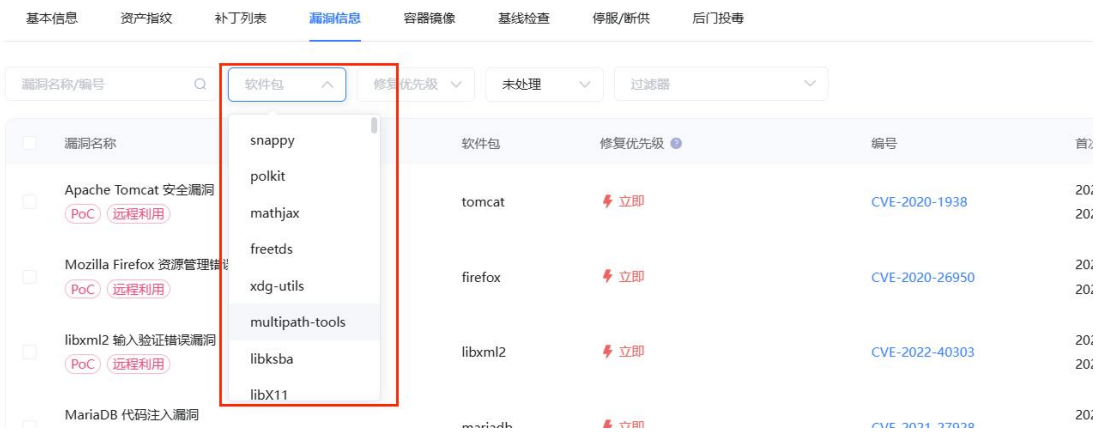


图 7：漏洞组件筛选

图 8：漏洞修复优先级

图 9：漏洞优先级得分

可以通过漏洞标签对漏洞进行分析，快速了解到受影响的漏洞属性，掌握漏洞的可被利用情况，如漏洞带有“PoC、远程利用、可被利用、本地利用、在野利用”这些标签说明可被利用性较高，需要尽快修复。还可以通过“官方补丁、修复版本、缓解措施”等标签筛选发布了对应修复措施的漏洞，帮助安全人员对漏洞进行修复。

图 10：漏洞标签分类

图 11：漏洞当前标签

指令集的修复方案：在检测结果页面，点击【漏洞信息】-【获取修复建议】，可查看智能修复建议，智能修复建议将同一软件的修复建议进行合并，并给出修复步骤，包含具体执行命令，根据这些指令可以快速实现漏洞批量修复。

图 12：指令集漏洞修复方案跳转指示

图 13：指令集漏洞修复方案

4、漏洞修复建议

在【漏洞信息】页面点击列表页的漏洞名称，可以看到单条漏洞的命中信息、修复建议（升级版本、安装补丁以及缓解措施），根据该指令能够快速准确、安全有效地对漏洞进行修复，解决漏洞可能造成的威胁和风险。

单条漏洞详情信息

在列表页点击漏洞的编号进入到漏洞的详情信息页面。在详情页面可以看到漏洞的标题、描述、PoC、影响范围、CPE、修复建议、缓解措施、CVSS、参考链接及漏洞图谱、相关漏洞、影响资产等相关信息。

图 14：漏洞详情信息

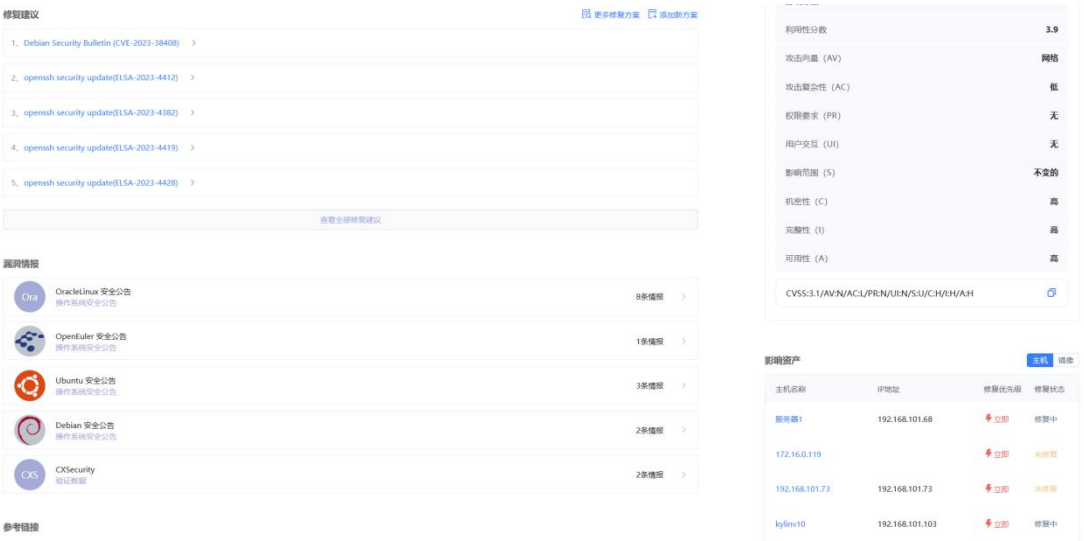


图 15：漏洞修复建议

图 16：单条漏洞基本信息跳转指示

图 17：漏洞信息

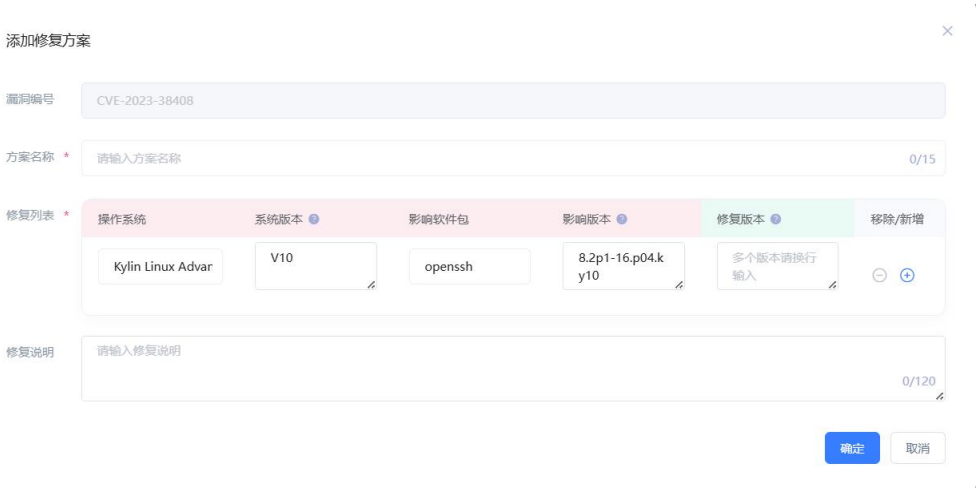


图 18：添加修复方案

利用工单管理漏洞处理流程

在【漏洞信息】页面，勾选漏洞，点击【将选中的未修复漏洞加入工单池】

图 19：将选入漏洞加入工单池

点击【工单池】，选择需要派单的漏洞，选择接收人，点击【去派单】

图 20：选择指派的工单

填写工单信息，点击【确定】工单派发成功。

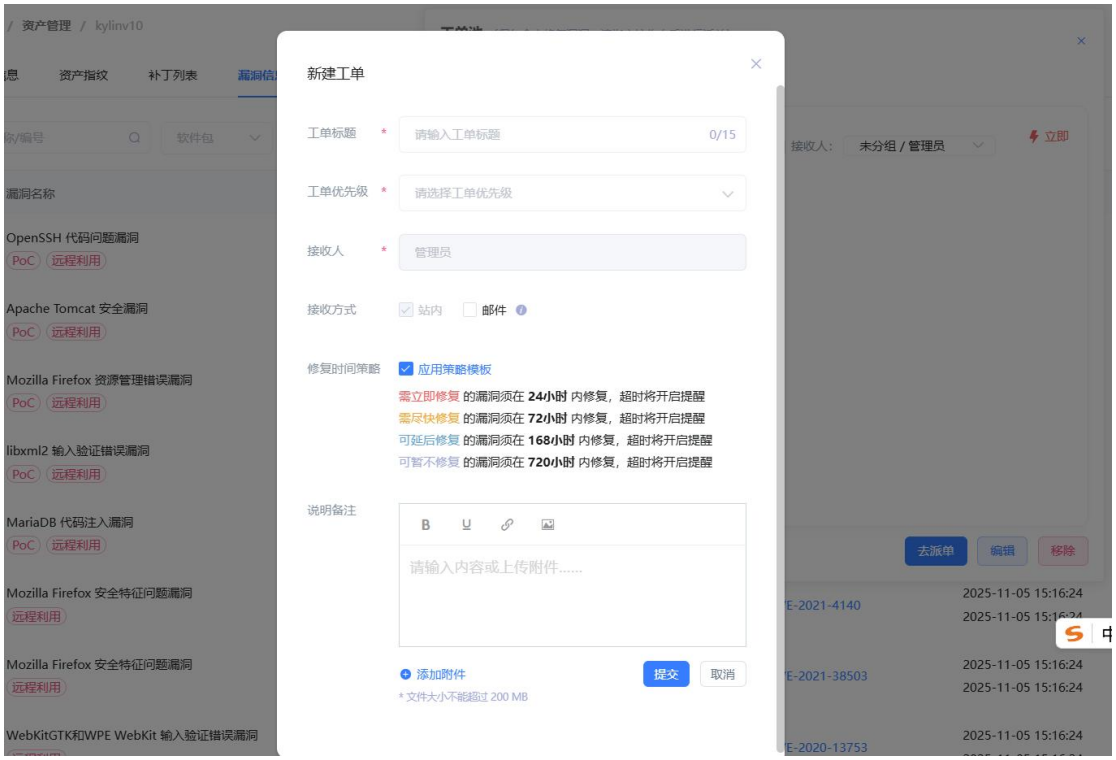


图 21：工单信息编辑

点击页面右上角工单图标选择工单，可通过【工单属性】中的工作状态来修改工单状态。在漏洞需要其他人协助时，可以通过【转派】给其他人来处理。

图 22：工单信息

麒麟操作系统漏洞检测实践（升鑫）

漏洞修补技术，也就是安全补丁，是最根本的漏洞解决方案。完整的补丁管理一般包含一下几个方面：现状分析、补丁跟踪、补丁验证、补丁安装、应急处理和补丁检查。这其中比较重要的是企业需要长期维护绿色、无污染的补丁源。

网络安全漏洞利用防范技术，主要针对漏洞利用触发利用条件进行干扰或拦截，本质上是一种漏洞缓解措施。主要技术有虚拟补丁、边界安全产品规则拦截，网络隔离，漏洞无效化等。

1、漏洞分析评估

（1）漏洞规则是否已更新至最新版本

漏洞规则的时效性是首先评估的内容，一般情况下建议每个月至少更新一次规则，保证新漏洞被及时发现，被替代漏洞及时更新到需修复的最准确版本；

（2）是否是误报漏洞

无论是扫描器还是 HIDS 扫描，都存在一定程度的误报，需要增加一定的人工确认环节。对于误报的程序可以进行加白处理。

（3）主机所属区域和业务组

实际生产过程中，企业一般都需要对自己的主机进行分组，有些组别内的主机承载着重要的业务系统，是需要着重关注其安全问题的。

（4）漏洞利用难度

实际评估过程中需要着重考虑评估漏洞的利用难度。如外网已经存在 EXP 利用脚本的远程利用漏洞更需要加紧修复，因为利用脚本的外网传播将会极大降低该漏洞的利用难度。

（5）漏洞危害程度

对于具有远程利用，本地提权，反序列化等特征的漏洞需要加强关注；对于影响面较大的漏洞需要格外关注，影响面较大，意味着黑客攻击的渗入内网后，可以通过相同漏洞，相同的手法再次获取更多主机的权限。

（6）漏洞的修复影响

实际生产过程中，安全人员经常会遇到很多漏洞，不知道修复顺序无从下手。那么评估漏洞修复的影响性就是其中必须经历的重要一环。可以将漏洞大致分为：“无需重启”、“重启系统”、“重启服务”三种，那么安全人员就会优先修复无影响的漏洞，以加快漏洞管理流程的流转。

2、规则更新操作步骤：

漏洞修复前，请首先检查漏洞检测规则的更新时间，一般情况下建议每月更新一次，其也与麒麟系统的普通漏洞更新频率相似，在确认规则无误后，可开始具体的检测修复工作；

如果出现紧急高危漏洞，可咨询安全厂商，尽快立即更新相关检测能力。进入后台-系统配置管理，登录后台；

图 1：系统登录

进入系统设置-规则更新功能，检查更新时间。

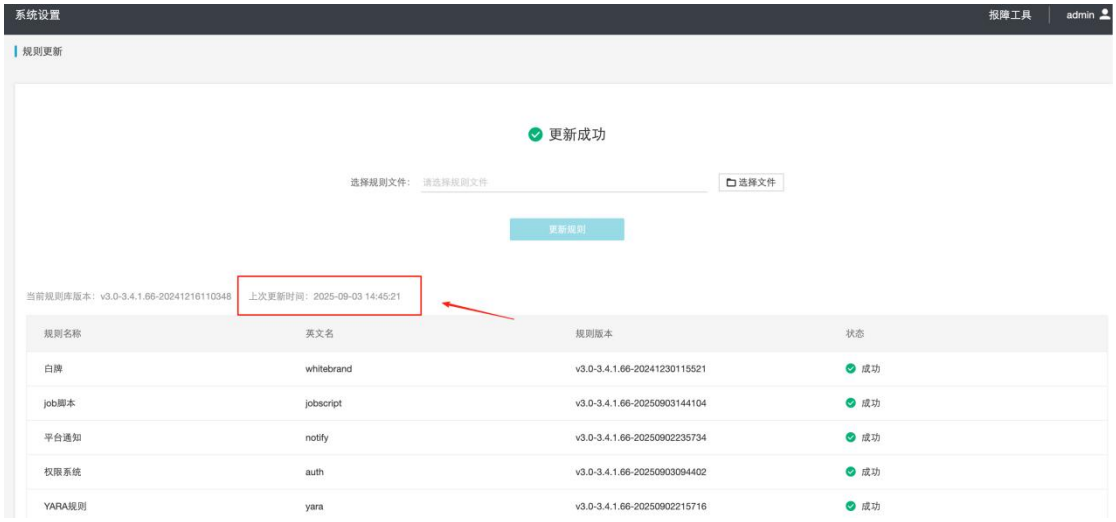


图 2：更新情况

（1）离线方式更新：使用离线规则包更新，如已超过常规更新时间，可向安全服务厂商申请获取最新规则更新包，上传更新；检查安全补丁，poc 规则包已经更新即可。

（2）在线自动更新：自动从公网获取规则，可参考安全厂商的相关方案，配置连接厂商的公网服务，自动更新漏洞检测规则；该方式在部分公网隔离的环境中不建议使用，其将导致对外网连接问题，务必与企业安全部门确认后再开启。

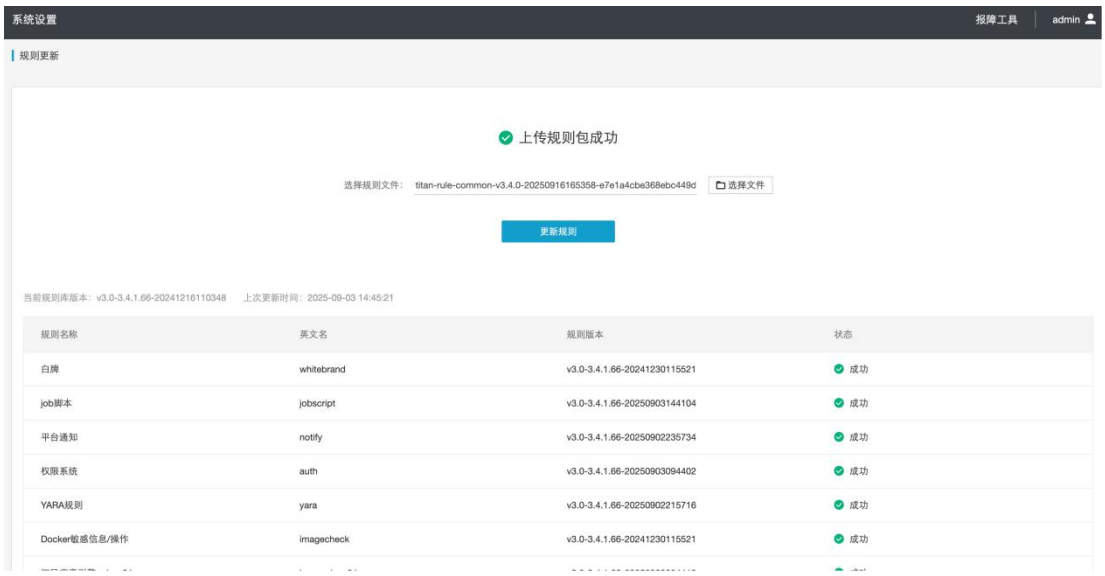


图 3：规则更新

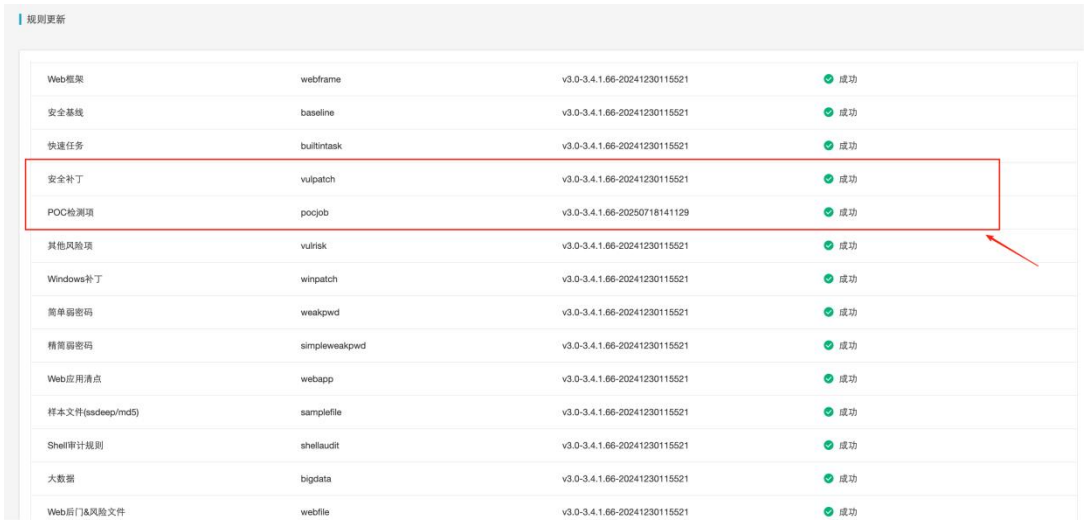


图 4：更新结果

3、漏洞修复措施和操作步骤：

通过清点主机上安装的应用、查找主机上正在运行的进程，找到对应的应用版本，与安全补丁库中的漏洞版本进行比对（本质就是版本比对），若该版本处

于漏洞版本范围内，则判断该主机上的该应用存在未打的安全补丁。补丁检测依赖系统安装包列表，不会检测非包安装的程序补丁。

漏洞检测：将漏洞检测规则下发到主机上进行执行，漏洞检测方式分为两种：POC 验证脚本和版本比对。

（1）POC 验证脚本检测方式：即通过漏洞 POC 脚本进行检测；服务端将 POC 脚本下发到 agent 主机上执行判断是否存在漏洞后进行上报。

（2）版本比对检测方式：即比对应用存在漏洞的版本来进行检测。

对于扫描出来的需要修复安全补丁。这类漏洞危害率更低，您可作为参考，建议–与业务人员确认后再做处理。

（3）处理方式：可以点击【补丁详情】或【影响主机数】的补丁详情来查看修复方法，从而修复安全补丁。

补丁详情：

图 5：风险信息

影响主机数–补丁详情：可在此查看修复建议的和修复命令，并且您可以自定义修复建议。

图 6：补丁信息

4、对于误报或已经修复补丁，可以对其进行加白操作，加白后将不再显示该补丁。

方法一：在安全补丁列表页选中要加白的补丁，点击【加入白名单】。10 秒后白名单生效，可在【白名单规则】中查看、编辑、删除加入白名单的补丁。

图 7：规则信息

方法二：在【白名单规则】页新建白名单规则，您需手动输入补丁条件列表，使用范围等信息。

图 8：白名单规则

5、漏洞检测

对于漏洞检测扫描出的漏洞，这类漏洞危害率更高，有极大的概率被攻击，建议您都进行修复。

（1）处理步骤：您可以在漏洞检测页或作业执行结果页，点击【漏洞详情】或【影响主机数】查看漏洞具体信息和修复建议，再按照修复建议对漏洞进行修复。

图 9：漏洞类型

漏洞详情：

图 10：漏洞详情

影响主机数：

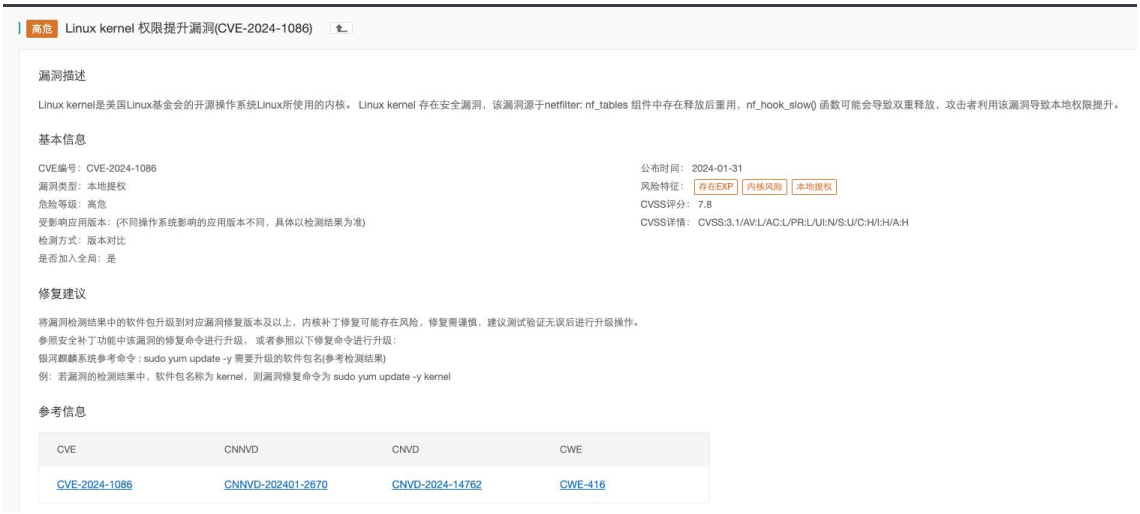


图 11：漏洞描述

对于无法修复的漏洞您可以联系厂商。

（2）对于误报或者已修复的漏洞，您可以将其加入白名单，加入白名单后将不再对其告警。

方法一：在漏洞列表页加入白名单，点击【加入白名单】，10 秒后白名单生效，可在【白名单规则】中查看、编辑、删除加入白名单的漏洞

图 12：漏洞白名单

方法二：在【白名单规则】页新建白名单规则，您需手动输入漏洞名，漏洞特征等信息。生效范围选择新数据表示白名单只对之后的漏洞生效，选择全部数据表示之前已检测出的该漏洞也移除漏洞告警列表。

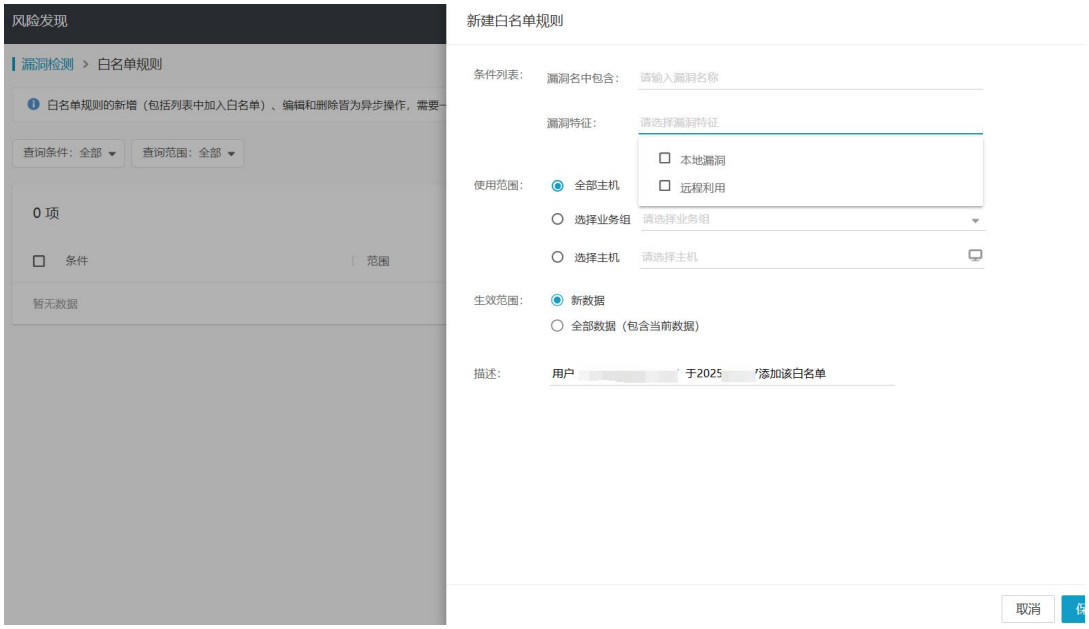


图 13：白名单规则

麒麟操作系统漏洞检测实践（绿盟）

1、绿盟漏洞扫描器工具配置与策略初始化

（1）扫描策略配置：首次启动扫描器后，需自定义扫描策略，设置扫描范围、深度、速度等参数，以满足不同业务场景的需求。

（2）初始化扫描引擎：首次使用时，必须初始化扫描引擎，加载最新漏洞库并更新扫描规则，确保扫描器能够准确识别最新的漏洞信息。

（3）创建扫描任务：

- 目标地址范围：创建扫描任务时，需明确指定目标系统的 IP 或域名范围，确保扫描的准确性。
- 排除列表设置：为避免误扫描，可设置排除列表，将不重要的设备或已知安全的系统排除在外。
- 执行周期安排：根据业务需求，设置扫描任务的执行周期，如每日、每周或每月，以保持对目标系统的持续监控。
- 任务命名与描述：为每个扫描任务设置清晰的名称和描述，使健于团队成员快速识别任务的归属与目的。

（4）执行扫描与进度监控：

- 扫描执行流程：扫描任务启动后，扫描引擎将依次进行端口探测、服务识别和漏洞检测，全面覆盖目标系统。
- 进度实时监控：扫描过程中，界面会实时显示已完成的主机数、发现的漏洞数、当前扫描的插件名称及预计剩余时间。
- 操作控制：用户可以根据需要暂停、继续或终止扫描任务，灵活调整扫描进度，以适应不同的业务需求。

（5）漏洞结果列表概览

- 漏洞分类汇总：扫描完成后，漏洞结果将按高危、中危、低危、分类汇总，方便快速定位关键问题。
- 筛选与排序：通过快速筛选栏，用户可以根据漏洞等级、关键字、时间范围等条件快速筛选漏洞，提升分析效率。

2、漏洞详情与修复建议

（1）漏洞详细信息

点击漏洞名称后，可查看漏洞描述、原理、CVE 编号、CVSS 分值及利用条件，全面了解漏洞细节。

（2）修复建议

扫描器提供官方补丁、配置加固、虚拟补丁等多种修复建议，帮助用户快速解决问题。

（3）修复验证

修复完成后，建议执行复扫任务，确认漏洞已成功关闭，形成完整的漏洞管理闭环。

（4）扫描优化建议

定期检查扫描性能指标，根据实际运行情况调整参数，确保扫描任务执行。

3、定期维护与更新

每周检查漏洞库更新并同步，每月清理历史任务日志，季度备份数据库与策略配置，确保扫描器持续稳定运行。

麒麟操作系统漏洞治理案例–脆弱性全过程管理方案：脆弱性全过程管理方案包含：漏洞发现、漏洞分析、漏洞处置、漏洞知识沉淀几个步骤。

图 1：漏洞修复流程

（1）漏洞发现

漏洞发现主要包含：全面漏洞发现、自动化智能扫描调度以及多源结果统一融合分析过程；

全面漏洞发现包含：对接绿盟扫描器、三方扫描器、威胁情报、渗透测试、风险评估结果人工录入；

多源结果统一融合分析包含:数据标准化、去重合并、黑白名单。

（2）漏洞分析

漏洞分析过程主要包含：优先级分析、变化趋势分析、漏洞验证、运维分析、排名统计、POC 扫描、风险分析报表管理等。

（3）漏洞处置

漏洞处置方式包括：多维画像、闭环处置、归档管理、工单管理、流程管理、通知管理、漏洞配置、知识库管理、分权分域以及资产分析等。

（4）漏洞知识沉淀

标准知识库：漏洞库、情报库、弱口令库、模板库、资产标记库；

运营经验库：指纹插件库、误报库、修复经验库；

（5）持续运营升级

麒麟操作系统漏洞治理案例–一个平台管理多视角资产台账。可实现一个平台管理多视角资产台账，过程包含：资质发现、资产分析、资产管理及资产画像。

图 2：资产画像

4、麒麟操作系统漏扫操作指南

以资产数据为核心，面向网络脆弱性管理，结合外部漏洞情报信息，在持续资产监控基础上，侧重风险优先级，整合多源脆弱性数据，聚焦关键风险，量化风险指标，提供漏洞全生命周期的管理方案。可以帮助客户建立快速响应、有序修补、持续优化的资产漏洞管理能力。

图 3：漏扫流程

麒麟操作系统漏洞检测实践（深信服）

登录云镜管理端，首页中切换导航菜单到[安全评估]，主要包括新建任务和任务列表两部分内容，任务主要包括全面扫描、资产发现、系统漏洞扫描、弱口令扫描、web 漏洞扫描、基线配置核查六个评估功能模块，任务列表展示所有历史和正在进行的任务。

在[安全评估]中，点击评估功能栏中的<系统漏洞扫描>进入到系统漏洞扫描的评估页面，如右图所示。其中，专项漏洞扫描包括：操作系统、网络设备、数据库等漏洞扫描，此外还可以选择紧急漏洞进行单独评估，如 Apache Log4j2 远程代码执行漏洞(CVE-2021-44228)。

在评估功能[系统漏洞扫描]页面上，点击功能栏<新建任务>跳转系统漏洞扫描的任务配置页面，如右图所示。

选择扫描模式，扫描模式有[基础扫描]和[专项漏洞扫描]两种。选择好扫描模式后进入系统漏洞扫描漏洞任务配置页面。

配置系统扫描漏洞任务的常规信息。点击<提交>，自动跳转到任务列表界面，完成系统漏洞扫描任务的创建。

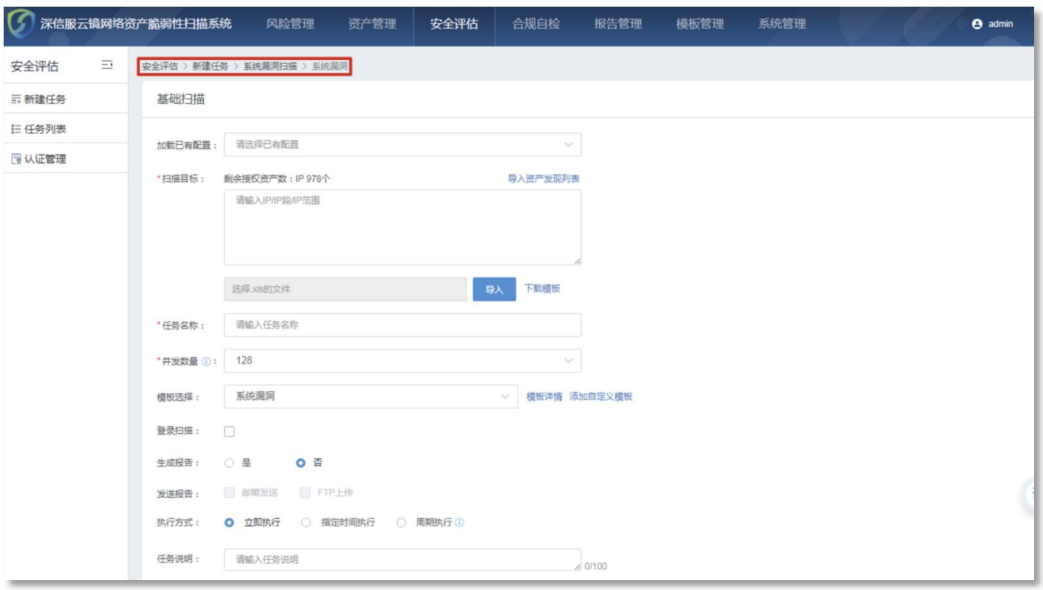


图 1：任务创建

图 2：扫描界面

表：扫描参数设置

参数	说明
加载已有配置	【可选操作】如果之前做过系统漏洞扫描，可以快速选取历史配置信息
扫描目标	【必选操作】支持通过如下方式配置扫描目标设备，最多可输入 10000 个字符进行输入，同时需要满足以下格式要求： 资产之间支持分号、逗号、换行符分割； IP 限制 1 个 B 段（256*256） IP 支持格式 192.168.1.6；200.200.1.1-15；192.168.0.0/16
导入	【可选操作】支持下载 excel 模板，填入资产目标信息后批量导入
任务名称	【必选操作】本次任务的名称，长度 2-100 个字符之间 **注意**：扫描任务较多的情况下，建议手动定义有区别的任务名称，完全依赖机器自动生成的任务名称，筛选度和可视度都不高
模板选择(基础扫描配置项)	【必选操作】当前扫描任务对应的漏洞扫描类型，默认模板为“系统漏洞”，根据需求自行调整，模板类型参考“系统漏洞模板”
登录扫描	勾选后需要配置资产登录账号密码，方便后面在其他模块中引用，如基线扫描核查

生成报告	【必选操作】默认不生成报告，可以手动点选生成报告。
发送报告	【可选操作】允许通过 FTP 或者邮箱发送报告。
执行方式	【必选操作】选择两种执行方式供之一： A：立即执行：提交任务后立即进入执行状态 B：指定时间执行：选择指定的时间点执行任务，精确到分钟。 C：周期执行：开启后，系统将定期按照任务扫描参数发起扫描，当到达扫描周期但是上次扫描未结束时，本次周期检测将被跳过； 按月执行时，如果当月没有此日，则在月末执行，如：选择每月 31 日执行，4 月没有 31 日，则在 30 日执行； 请尽量对小批量扫描目标开启周期检测，避免单任务扫描时间过长，影响后续周期扫描时间。
任务说明	【可选操作】任务备注说明
高级配置	包括： 存活性探测策略 端口扫描策略 低可信度漏洞扫描 Web 应用扫描

麒麟操作系统漏洞检测实践（猎鹰安全）

猎鹰终端安全管理系统 V9.0 是一款终端安全防护产品，支持病毒查杀、漏洞修复、桌面管理、资产管理、终端合规检查、边界防护、日志审计、终端运维管理等功能，实现终端整体安全防护。同时终端防护产品也支持与防毒墙、威胁检测平台等安全设备联动协同，形成高效的主动式的统一安全防护体系，是一款一站式终端安全管理的产品。采用业界主流的 B/S 开发模式，由系统中心（集成了管理平台、升级服务及云查杀引擎）及客户端组成了终端安全防病毒安全保障体系。

漏洞扫描分为主动智能扫描和客户端独立扫描两种方式。普通用户可以通过本机的客户端手动进行漏洞扫描和安装修补程序。管理员可以通过系统中心控制台来查看局域网内所有的客户端主动智能上报的漏洞信息，再根据漏洞补丁信息选择需要安装的终端，并通知其下载和安装修补程序。

1、安全概况

统计已部署终端的弱密码信息、服务信息、已安装补丁信息、端口信息，可以清晰知终端资产态势，便于及时发现弱势，避免被攻击。

（1） 弱密码信息

通过本地后台计算，统计已部署终端的弱密码信息，如果命中则上报到管理平台。

图 1：弱密码信息

（2）服务信息

统计已部署终端的系统服务信息，方便管理员及时掌握全网终端环境信息。

图 2：服务信息

（3）已安装补丁信息

用以统计内网已部署终端补丁安装情况。

图 3：补丁信息

（4）端口扫描信息

统计内网已部署终端本地操作系统端口开放情况。

图 4：端口扫描信息

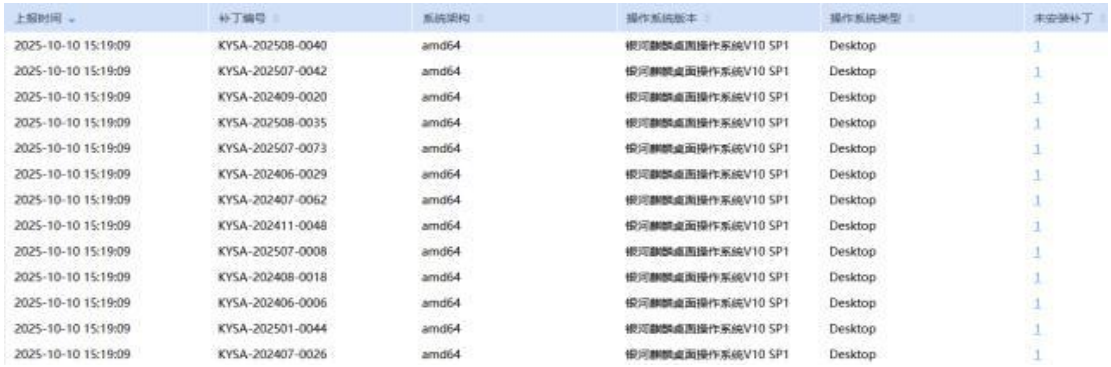
2、漏洞修复

具有独特的漏洞扫描自动检测软件各种漏洞，同时提供官方补丁下载地址，从根本上减少安全隐患。

（1）按补丁查看

【漏洞修复】--【按补丁查看】

- 支持按补丁类别进行查看。
- 支持分组查看。
- 显示补丁详细信息以及未修复终端主机信息



上报时间	补丁编号	系统架构	操作系统版本	操作系统类型	未安装补丁
2025-10-10 15:19:09	KYSA-202508-0040	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202507-0042	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202409-0020	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202508-0035	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202507-0073	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202406-0029	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202407-0062	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202411-0048	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202507-0008	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202408-0018	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202406-0006	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202501-0044	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1
2025-10-10 15:19:09	KYSA-202407-0026	amd64	银河麒麟桌面操作系统V10 SP1	Desktop	1

图 5：按补丁查看界面

（2）按终端查看

【漏洞修复】--【按终端查看】

- 支持对目标计算机进行漏洞查看。
- 支持对目标分组漏洞信息查看。

图 6：按终端查看界面

3、报表管理

支持对终端病毒日志、安全日志、漏洞修复、僵木蠕虫病毒、终端防护日志、文件及应用升级日志、终端事件告警、管理员日志及云查杀等信息进行报表统计。能够从终端、全网、分级、分组等多维度,以及图表、数据等多视图角度进行统计与展现,也能按月、季、年的时间维度进行趋势分析,同时支持报表的订阅、导出及打印,帮助管理员对日常安全防护、安全运维工作进行分析评估。

（1） 漏洞报表

记录全网终端计算机补丁的未安装数/已安装数/有漏洞的终端数/高危漏洞修复数/未装补丁按 OS 统计等的情况进行审计、统计、排名，并查看走势。

- 查看本级以及下级的补丁安装/未安装数报表和漏洞/高危漏洞修复报表。
- 支持关键字、时间段、组织范围、事件类别及状态等属性进行快速检索。
- 全网终端补丁安装的统计、排名、走势以图形化展示支持查看对应明细。
- 支持报表导出 ，支持报表导出，支持 CSV、PDF、PNG 等格式报表。

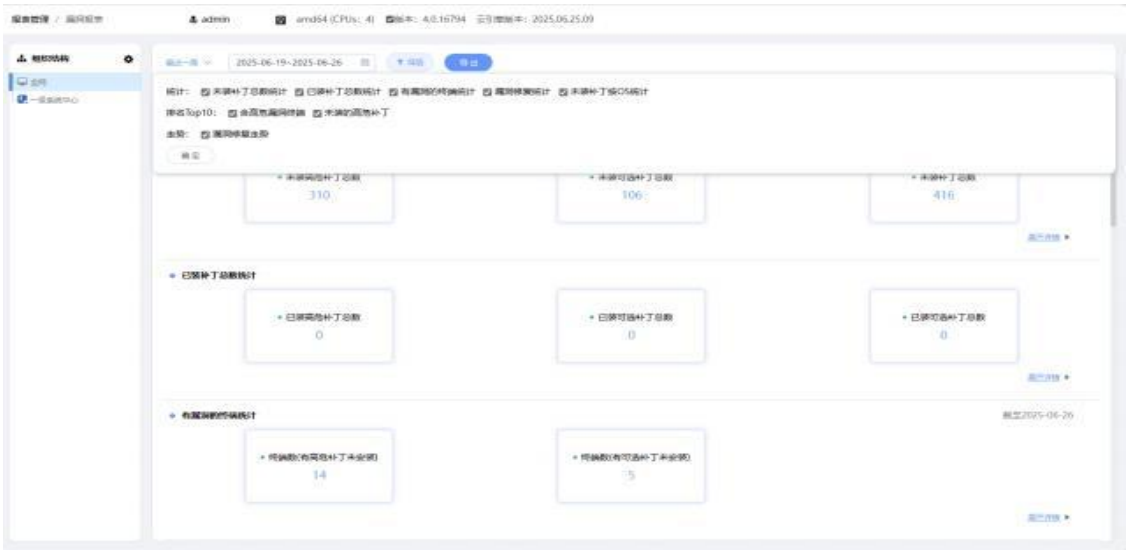


图 7：漏洞报表界面

（2）终端统计

- 未装补丁总数统计：统计各分级未安装的补丁（包括高危补丁、可选补丁）；
- 已装补丁总数统计：统计各分级已安装的补丁（包括高危补丁、可选补丁）；
- 有漏洞的终端统计：统计各分级未装高危补丁的终端数及未安装可选补丁的终端数；
- 高危漏洞修复统计：统计具体高危漏洞在全网被修复的次数。
- 漏洞修复走势：展示一段时间安装的高危补丁数和安装的可选补丁数总和。

（3）漏洞日志

终端在某个时间点修复的补丁类型及修复结果明细详情 ，可选类型导出日志；根据修复结果，修复成功、安装失败、下载失败情况导出日志。支持按时段、分组、关键字等过滤显示。

4、设置中心

设置中心是配置项的汇总 ，用于中心的配置以及终端可执行指令，提供统一对账号管理、多级管理、终端安全策略以及升级设置等进行设置管理【设置中心】--【系统中心】--【系统设置】--【全局设置】。

自动升级设置：开启自动升级操作系统补补丁库信息。

图 8：升级设置

5、Linux 终端

打开终端 ，首页为用户展示最近发现病毒数、隔离区文件数量、CPU 内存占用率以及当前系统时间和电脑开机运行时间。并且提供快速查杀访问入口。

图 9：Linux 终端首页

终端用户可通过补丁信息查看当前操作系统未修复、已修复漏洞信息以及相关补丁详细信息描述。

图 10：漏洞补丁信息

6、漏扫工具 FAQ

（1）为何不能访问 Web 界面?

- 是 https 连接，而不是 http
- 检查防火墙 6868 端口是否放开

（2）Web 看不到终端信息?

- 检查终端 ip 指向是否正确
- 检查防火墙 5688 端口是否放开

（3）漏扫结果中部分资产没有漏扫记录?

- 终端每日会自动执行漏洞扫描任务，扫描任务无需人为干预，只需要主机处于开机状态。
- 如果仍缺失扫描记录需要检查漏扫工具服务是否正常 ，或联系厂商对接。

（4）出现漏扫误报怎么处理?

需确保管理中心漏扫补丁库是否更新最新版本。

处理措施:

- 外网环境：检查是否开启{设置中心-系统中心-全局设置-自动升级 Linux 补丁库}策略
- 内网环境:需联系厂商指导或自行从 https://update_xc.ejinshan.net/获取离线升级数据并导入。

需确保终端到管理中心 5688 端口通讯正常。

- 终端通过该端口从管理中心获取最新漏洞库,重新进行漏洞扫描并上报更新结果。

（5）漏扫工具是否提供手动修复方法?

- 漏扫工具在获取最新漏洞库后扫描的结果输出，可在修复详情中查看详情，包含手动修复方法，或对接厂商进行指导修复。

麒麟操作系统漏洞检测实践（哨云）

哨云景御云检测与响应系统依托云平台原生能力与 API，全面采集并分析云环境中的数据存储、事件日志、网络流量及配置信息，能够快速识别公有云、私有云、虚拟化及容器等平台及其承载应用系统中存在的漏洞、弱密码、配置错误等安全风险。系统结合 AI 攻击建模技术，并基于资产关键性与业务影响等多维度分析，自动构建风险量化模型，智能生成修复优先级清单，从而协助安全团队优先处置最关键的安全威胁，提升整体安全响应效率。

1、检查任务下发

哨云景御由两部分组成：管理中心和云连接器，管理中心是基于 Web 的集中式管理系统，安全管理员可以通过它配置安全策略，查看和处置风险；云连接器则负责同步所有云资产，统一调度对云主机的安全检测、响应处置等任务。所以部署完成后一定要确认云连接器是否正常部署和配置，云连接器的状态需要是正常。

图 1：状态显示

哨云景御支持自动扫描和手动扫描，也可以根据实际业务需要，在特定时间针对特定主机下发扫描任务。如果仅需漏洞扫描，选择快速扫描指定主机即可。

图 2：检查操作系统

图 3：基本设置

2、漏洞分析

哨云景御的漏洞检测机制在匹配组件版本的基础上，深度融合配置信息分析，并引入资产关键性与业务影响等多维度数据，通过攻击面管理与路径预测技术，评估漏洞的真实风险及处置优先级，既提升了漏洞检测准确率，又能帮助运维人员聚集解决最关键的安全风险。

图 4：攻击路径

图 5：主机信息

扫描完成后，可以在管理中心页面中，通过“主机视角”和“漏洞视角”查看完整的漏洞信息和受影响软件及具体版本情况。漏洞详情描述页面也能看到主流操作系统厂商，包括麒麟软件对该漏洞的描述及分析。

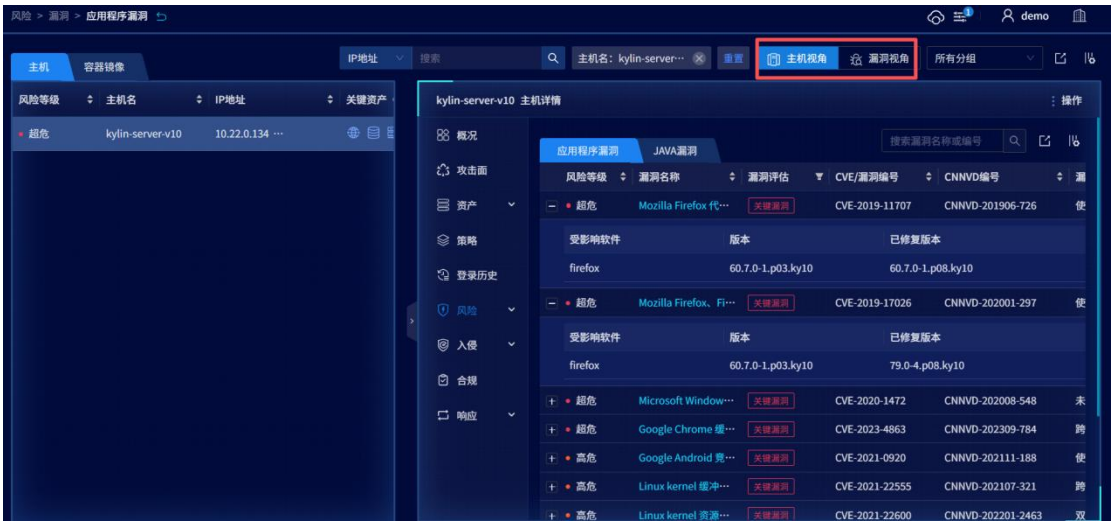


图 6：漏洞信息

图 7：漏洞详情

3、漏洞误报处理

如果经研判后发现某漏洞确实存在误报，可以直接在处置任务中点击误报直接处置。

对于已确定某策略误报高，经评估不需要检测时，可以在自定义策略中删除或禁用该策略或者通过加白名单的方式，下次检测不再调用该策略。

图 8：策略信息

4、报告输出

哨云景御系统内置各种报表模版，支持按月、按天、按周等不同周期频率要求手动或自动生成安全巡检报表，并可以 PDF、Excel、HTML 等各种形式导出，方便查看。

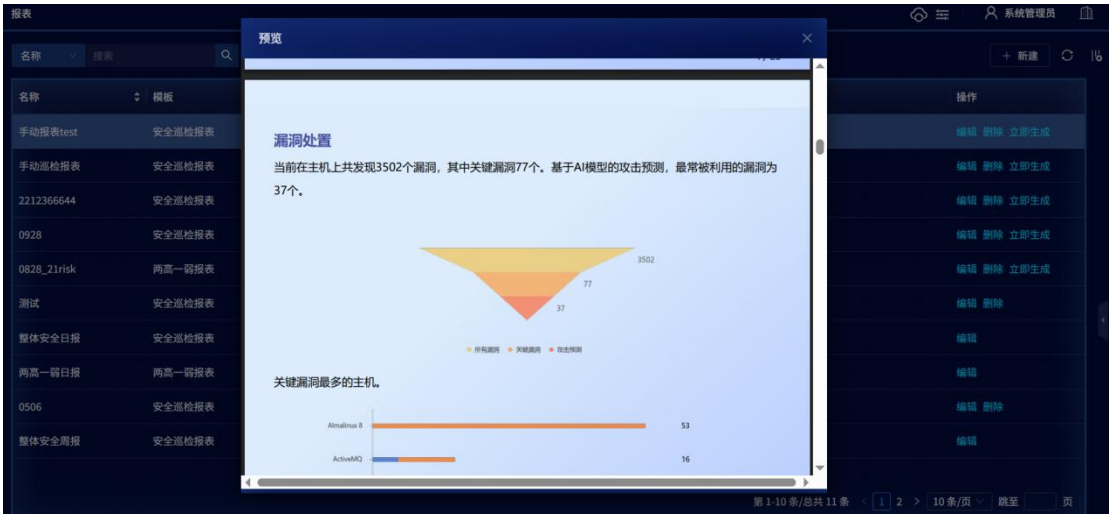


图 9：报告输出