



UXSINO
优炫软件

Release Notes

CDPS Release 2.0.5.4

【文档发布】

文档名称	Release Notes		
编写部门	北京优炫软件股份有限公司		
适用对象	公司技术人员、实施人员，合作单位技术人员		
编写	马志伟	审核	马志伟
文档版本	V1.0	发布日期	2021.10.16

【适用范围】

该发布说明适用于优炫操作系统安全增强系统 V2.0.5.4

【修订记录】

序号	修订章节	修订内容	修订人	修订日期
01	V1.0	文档初建	马志伟	2021.10.16

目 录

1	发布内容.....	1
2	新增功能/优化内容.....	1
2.1	新增功能.....	1
2.2	优化内容.....	2
3	已解决问题（严重问题）.....	3
3.1	Windows 问题列表.....	3
3.2	Linux 问题列表.....	6
4	参考文档.....	21

1 发布内容

优炫操作系统安全增强系统 V5.4 发布清单如下表所示：

表 1-1 CDPS 5.4 发布清单

发布内容	获取路径
Linux 安装包	http://cd.uxsino.com:24080/f/2192185 → ver2.0.5.4
Windows 安装包	http://cd.uxsino.com:24080/f/2192185 → ver2.0.5.4
白皮书	http://cd.uxsino.com:24080/f/2316572 → doc
测试报告	http://cd.uxsino.com:24080/f/2316572 → doc
用户操作手册	http://cd.uxsino.com:24080/f/2316572 → doc
版本说明文档	http://cd.uxsino.com:24080/f/2316572 → doc
安装卸载指南	http://cd.uxsino.com:24080/f/2316572 → doc
对外测试大纲	http://cd.uxsino.com:24080/f/2316572 → doc
招标参数	http://cd.uxsino.com:24080/f/2316572 → doc
销售一指禅	http://cd.uxsino.com:24080/f/2316572 → doc
验收方案	http://cd.uxsino.com:24080/f/2316572 → doc
CDPS 5.4 新功能介绍【视频】	http://cd.uxsino.com:24080/f/2316572 → 功能介绍视频

2 新增功能/优化内容

2.1 新增功能

- 1) 资源管理模块新增设备发现功能；
- 2) 资源管理模块新增设备发现功能；
- 3) 新增 Webshell 后门检测功能；
- 4) 新增恶意代码查杀功能；
- 5) 模板管理模块新增中间件基线模板功能和数据库基线模板功能；安全基线、数据库基线、中间件基线共存；
- 6) 新增主机弱口令检测功能，检测主机用户密码强弱，新增弱口令字点模块；

- 7) 弱口令检测模块新增 mysql 弱口令检测功能;
- 8) 远程安装、卸载 agent;
- 9) 统计分析模块新增安全态势统计和安全态势统计图功能,能更好的展示安全方面的违规记录;
- 10) mysql 数据库、用户弱口令检测,弱口令字典升级;
- 11) Linux 增加反弹 shell 功能;
- 12) Linux 新增防 CC 攻击;
- 13) Linux 新增入侵检测(非法 IP 登录检测、非法账号登录检测、反弹 shell 检测);
- 14) Windows 入侵检测模块新增防爆力破解、非法 IP 登录检测、非法账号登录检测功能;
- 15) Windows 新增漏洞扫描和补丁检测功能;
- 16) Linux 主机用户列表新增 root 权限、sudo 权限、最后登录时间、公钥 key 等列。

2.2 优化内容

- 1) 防暴力破解支持三态开关;
- 2) cpu/mem 超过阈值 ListenHostServer 自动休眠;
- 3) Linux 防火墙设置:一键丢弃、一键接受所有端口(仅支持 redhat/Centos7);
- 4) Linux 安装前环境检测;
- 5) 设置系统程序白名单;
- 6) 首页新增风险趋势;
- 7) 主机用户列表支持显示/隐藏系统用户;
- 8) 告警中心:隐藏已删除站点告警;
- 9) 拓扑展示:删除离线站点时可选同时删除该站点告警信息;
- 10) 优化资源管理--全部资源页面;升级了特征库下发功能,增加了病毒库、弱口令字典、补丁包的下发功能;
- 11) 优化告警中心告警消除功能、增加了告警等级种类,可以一键消除所有未消除的告警信息;
- 12) 优化用户安全策略,会根据用户显示所有类型的违规记录;
- 13) 剩余信息清除功能改造,可导入带通配符路径;
- 14) 文件完整性检查功能改造,支持递归;
- 15) 许可证管理-采集许可证信息增加授权信息列;
- 16) 拓扑首页增加超时机制,超时 1 小时退出登录;

- 17) U 盘白名单参考安全终端设计，去掉主机可信 U 盘管理页面，将已下发 U 盘策略管理功能合到 U 盘白名单开关；
- 18) 重启自动加载安全内核；
- 19) 去掉远程登录功能。

3 已解决问题（严重问题）

3.1 Windows 问题列表

Windows 操作系统，共发现严重问题 84 个。

表 3-1Windows 问题列表

Ticket	跟踪	主题
117029	缺陷	【恶意代码查杀】快速查杀按钮不能用，若没有什么价值，可以去掉
116686	缺陷	【恶意代码查杀】病毒查杀过程中切换页面，查杀完成后管理端页面卡死
121094	缺陷	【管理端卸载】卸载后有残留文件
121091	缺陷	【资源管理】链接途径不能下载代理端安装包
121088	缺陷	【Web5.4_checklist】可用内存实际结果和检测结果都不对
121069	缺陷	【恶意代码查杀】-隔离文件取消隔离，信任文件取消信任
121068	缺陷	【防火墙】添加只有协议的防火墙规则失败
121048	缺陷	【防火墙】-目的端口选填项失效
121032	缺陷	【漏洞扫描】查看扫描结果详情页面无响应
120643	缺陷	【CDPS 关闭浏览器后再打开 可不经登录直接进入上一次关闭页面】
120112	缺陷	【WinXP sp3 Listenserver 挂死】下发策略后重启主机,Listenserver 挂死
120109	缺陷	【安全基线】选中加固后重启代理端一键扫描卡死
120106	缺陷	【通信】安全基线选中加固后重启代理端主机管理端连接不上代理端（无 4611 端口，偶现）
119579	缺陷	【恶意代码查杀】点击暂停按钮后再点击终止按钮，浏览器崩溃，再次登录连接站点报通信异常
118819	缺陷	【Listenserver_内存泄漏】连续运行 4 天左右，Listenserver 内存上涨到 200M 左右

118748	缺陷	【日志管理】病毒扫描和 WebsHELL 后门检测没显示具体数量的日志记录
118716	缺陷	【恶意代码查杀】执行终止操作后再次执行全盘查杀出现异常
118711	缺陷	【恶意代码查杀】扫描等待窗口疑似卡死
118281	缺陷	【漏洞扫描】执行漏洞扫描无扫描结果
117854	缺陷	【非法外联】代理端能上外网的情况下打开非法外联开关同网段 IP 地址 ping 不通
117817	缺陷	【恶意代码查杀】全盘查杀失败
117373	缺陷	【代理端卸载】需提供卸载命令或卸载程序
116724	缺陷	【恶意代码查杀】下发病毒库文件失败
115009	缺陷	【CDPS 安全基线加固无法生效】
114934	缺陷	【防火墙】关闭端口打开非法外联开关防火墙默认规则变成 4 条
114726	缺陷	【非法外联】能上外网的前提下打开非法外联开关打开防火墙控制的端口使得代理端主机物理断网，关闭非法外联开关后仍然无法上外网
114307	缺陷	【防火墙】IPv6 地址 ICMP 协议没有符合接受优先规则
114224	缺陷	【防暴力破解】可信地址 ssh 访问代理端达到限制次数产生防暴力破解日志
114105	缺陷	【防暴力破解】使用管理端 Ip 对代理端进行暴力破解达到设置次数后管理端 IP 自动添加黑名单导致拓扑失败
113798	缺陷	【升级病毒特征库】升级病毒特征库失败
113781	缺陷	【漏洞扫描】漏洞扫描没有结果
113083	缺陷	【防暴力破解】设置防暴力破解黑名单时系统不响应，管理端无法重新登录
113076	缺陷	【2016_Listenserver】重启主机后，Listenserver 进程 CPU 高达 90+
113075	缺陷	【恶意代码查杀】模式一和模式二的病毒检出率不一样，且有时会扫描失败
113069	缺陷	【安装部署】下载代理端安装包时系统报 404
113065	缺陷	【IPV6 弱口令检测】使用 IPV6 新建数据库信息失败
112932	缺陷	【防暴力破解】下发非法 IP 登录非法账号登录开关使防暴力破解黑名单失效
112028	缺陷	【websHELL 后门检测】文件处于打开的状态时执行扫描无法被扫描到
111955	缺陷	【恶意代码查杀】病毒文件打开的情况下无法隔离和清除
111773	缺陷	【恶意代码查杀】同一个文件夹采用模式一和模式二扫描出来的结果

		不一样
111581	缺陷	补丁库升级失败
111203	缺陷	文件强防，用户等级大于文件等级，cmd 命令删除文件成功
110974	缺陷	【恶意代码查杀】采用模式二扫描后取消隔离失败文件消失
110963	缺陷	【恶意代码查杀】将隔离的文件取消隔离后重新扫描文件没有被扫描出来
110946	缺陷	【恶意代码查杀】打开防病毒开关后代理端隔离文件夹可以访问
110541	缺陷	【安全开关控制】USB 无线网卡拦截开关开启后代理端无线网卡没有被禁用
110509	缺陷	【安全开关控制】非法外联开关开启后代理端可以上网（IPV4）
110250	缺陷	【websHELL 后门检测】扫描结果不正确
110146	缺陷	【WebShell 后门检测】信任的文件重新扫描后变成未处理
110079	缺陷	【防病毒】防病毒扫描需增加两种扫描模式
110074	缺陷	【许可证管理】导出的授权压缩包里没有授权文件
110072	缺陷	【许可证管理】IP v6 地址显示错误
110070	缺陷	【许可证管理】管理端许可证信息中存在空数据导致无法导出记录
110034	缺陷	【安全策略管理】Windows 系统开关中防暴力破解开关无法设置为 ON
109998	缺陷	【IE 浏览器】IE 浏览器频繁出现崩溃现象
109954	缺陷	【许可证管理】采集许可证信息页面不显示主机许可证信息
109863	缺陷	【代理端安装】WhiteListInit 停止工作
109847	缺陷	【安全基线 59 项_删除默认的路由配置】卸载代理端会清除掉网关
109839	缺陷	【弱口令检测】弱口令字典升级失败
109822	缺陷	【通信问题】执行连接站点操作时系统报通信异常
109775	缺陷	【代理端】2016 代理端主机 CPU 近 100%
109745	缺陷	【防暴力破解】IPv6 地址加入黑名单没有生效
109717	缺陷	【性能】CPU 内存异常
109648	缺陷	【防暴力破解】超过暴力破解的次数后 IP 没有加入到黑名单
108515	缺陷	【弱口令检测】修改数据库信息失败，点击取消后，界面显示异常
108427	缺陷	【病毒扫描】病毒扫描失败_全盘扫描
108021	缺陷	【资源管理】设备发现无法扫描到代理端 IPV6 地址
107999	缺陷	【退出】点击退出按钮 IE 停止工作
107965	缺陷	【防火墙】Win7 系统蓝屏
107776	缺陷	【风险趋势】将病毒清除后病毒扫描信息没有减少反而增加

107758	缺陷	【模板管理】资源池配置中的筛选条件为基线类型时，搜索结果都为空
107747	缺陷	【弱口令检测】未升级弱口令检测结果显示弱，升级弱口令后检测结果显示强
107718	缺陷	【风险趋势】病毒扫描数据与病毒查杀结果不一致
107605	缺陷	【首页】登录管理端后在首页放置一段时间没有操作 IE 停止工作
107236	缺陷	【端口管理】关闭端口时防火墙开关会被打开
107222	缺陷	【端口管理】打开端口时会开启防火墙开关（技术反映的）
107091	缺陷	【资源管理】主机移动到自定义组后，等待段时间刷新后，主机又回到默认分组中
107036	缺陷	【主机用户管理】新增主机用户登录密码为空时，密码状态判断为强密码
106832	缺陷	【现场项目提交】Windows 代理端卸载后文件目录有残留，再次安装无法继续，需要给残留目录赋予权限后才能删除目录并继续安装
106830	缺陷	【现场项目提交】Windows 代理端卸载后注册表中仍有残留
106815	缺陷	【安装部署】点击新建，系统选项里没有 Windows 系统
106809	缺陷	【现场项目提交】告警中心、实时告警、日志三者中的信息不同步
106807	缺陷	【现场项目提交】Windows 代理端不支持授权到期前 30 天告警
83871	缺陷	【文件完整性检查】系统中有两个入口是做完整性检查的，检查的结果会存在不一致的情况

3.2 Linux 问题列表

Linux 操作系统，共发现严重问题 273 个。

表 3-2Linux 问题列表

Ticket	跟踪	主题
116755	缺陷	ver2.0.5.4a15: 白名单开关打开后执行代理端安装脚本主机卡死，并且通信异常
115290	缺陷	ver2.0.5.4a13:web 页面打开安全开关后再初始化系统白名单不生效等问题
115233	缺陷	ver2.0.5.4a13_redhat 6.5: 安装代理端提示/opt 磁盘被占满，查看 /bin/su 文件为空，导致 su 功能失效
113253	缺陷	ver2.0.5.4a10_CentOS7.2 64 位: 手动执行 rmmmod uxcdps 时主机崩溃重启

112723	缺陷	ver2.0.5.4a10_中国移动: 病毒查杀过程中, 代理端主机重启
112613	缺陷	ver2.0.5.4a10 64 位_Centos7.9: 执行稳定性测试 1min, 机器异常重启
111605	缺陷	ver2.0.5.4a6_Redhat5.8 实体机: 执行稳定性不到 24 小时, 代理端不可用
107221	缺陷	ver2.0.5.4a5_Centos7.4 64 位: 实体机上稳定性脚本执行代理端机器会重启
121124	缺陷	ver2.0.5.4a22_CentOS7.2: pgadmin 连接状态下开启反弹 shell 开关时代理端进程崩溃
121122	缺陷	ver2.0.5.4a22: IPV6 执行反弹 shell 后代理端服务挂掉
120741	缺陷	ver2.0.5.4a21_redhat7.2: 程序白名单页面, 扫描后查看 10w+ 文件 server 服务启动失败
120622	缺陷	ver2.0.5.4a21 64 位_Redhat6.5: 使用 icmp flood 进行 dos 攻击, 代理端 server 服务端口被占用, 服务一直起不来
120511	缺陷	ver2.0.5.4a21: 病毒查杀终止后再次查杀结果有误
120501	缺陷	ver2.0.5.4a21: 恶意代码查杀终止后相应进程不立即退出
120474	缺陷	ver2.0.5.4a21_CentOS7.2: 主机执行 reboot 时代理端异常产生 core 文件
120438	缺陷	ver2.0.5.4a21_CentOS7.2: 添加程序白名单过程中手动 kill 代理端进程后 server 进程异常
120437	缺陷	ver2.0.5.4a21: 反弹 shell 打开时进行病毒扫描会产生反弹 shell 告警
120435	缺陷	ver2.0.5.4a21_CentOS7.2: 通过文件列表查看包含 10w+ 文件的目录时代理端退出
120419	缺陷	ver2.0.5.4a21_bcLinux7.4: 漏洞扫描失败
120351	缺陷	ver2.0.5.4a21_redhat7.4: 关闭一次程序白名单开关, 启动一个 watchdog 进程
120348	缺陷	ver2.0.5.4a21: 通过 web 端设置系统白名单时提示失败
120347	缺陷	ver2.0.5.4a21: 打开白名单开关一分钟左右, 产生很多白名单告警
119863	缺陷	ver2.0.5.4a19: 防暴力破解规则为代理端自身 IP 时且设置限制时, server 每隔 7 分钟被 kill
119819	缺陷	ver2.0.5.4a19_redhat7.2: 白名单开关关闭, 告警中心还会产生白名单告警

119815	缺陷	ver2.0.5.4a19_Centos7.9 64 位：开启 USB 光盘存储开关，连接 USB 外接光驱未被移除
119812	缺陷	ver2.0.5.4a19_redhat7.2:防暴力破解选择 IP 黑名单,实际还可 ssh 连接成功
119753	缺陷	ver2.0.5.4a19-文件完整性检查:选中文件重新生成md5 报程序异常,管理端无响应,重新登录后连接栈点报:通信异常
119425	缺陷	ver2.0.5.4a19_redhat6.8:病毒会自动进行扫描
119423	缺陷	ver2.0.5.4a19-端口设置:选中所有端口,点【选中打开】后,管理端响应不过来,刷新浏览器重新连接栈点报:通信异常
119420	缺陷	ver2.0.5.4a19:程序白名单列表显示后点击尾页和全部选择时代理端异常退出
119419	缺陷	ver2.0.5.4a19_centos5.7:漏洞扫描响应扫描完成,前端页面超 30 分钟一直显示加载数据
119391	缺陷	ver2.0.5.4a19_redhat7.2:打开反弹 shell 开关, telnet 远程连接成功, server 挂掉且重启失败
119375	缺陷	ver2.0.5.4a19-防火墙:通过代理端设置规则后,SSH 丢弃规则没有生效
119362	缺陷	ver2.0.5.4a19_bclinux7.4:防暴力破解开关为 ON 时新建 IP 黑名单限制和可信失败
119351	缺陷	ver2.0.5.4a19:代理端高概率被 watchdog 杀死
119327	缺陷	ver2.0.5.4a19:文件完整性检查后,管理端没响应,刷新浏览器后管理端退出
119316	缺陷	ver2.0.5.4a19:卸载代理端时管理端服务也被杀死(单机版)
119298	缺陷	ver2.0.5.4a19_bclinux7.4:打开安全开关和强访开关后, server 和 watchdog 异常退出(偶现),无 core 文件产生
119288	缺陷	ver2.0.5.4a19_CentOS7.2 64 位:popup 进程不能自动启动
119281	缺陷	ver2.0.5.4a19:webshell 扫描提示失败
119276	缺陷	ver2.0.5.4a19_centos7.9_64 位:打开反弹 shell 开关,管理端页面显示通信异常,代理端 server 服务重启
119275	缺陷	ver2.0.5.4a17_Redhat6.8:打开所有开关后页面卡住(除了反弹 shell 开关)
119254	缺陷	ver2.0.5.4a19:代理端卸载后不删除隐藏 license 文件情况下再重装授权信息均显示为 0

118879	缺陷	ver2.0.5.4a17_redhat5.6 64 位: 修改弱口令文件中的内容后, 重新导入, 用户的密码状态和更新后的弱口令字典内容对不上
118849	缺陷	ver2.0.5.4a17_CentOS7.2 64 位: 测试过程中 su 文件大小变化且在内核开启情况下无法恢复正常
118845	缺陷	ver2.0.5.4a17: 当/var/log/目录下存在 messages.bak 或 secure.bak 文件时, web 界面系统日志、安全日志显示不正确
118826	缺陷	ver2.0.5.4a17: 反弹 shell 开关打开后会拦截通过终端方式访问常用的一些端口服务
118817	缺陷	ver2.0.5.4a17: webshell 扫描成功后再次点击文件列表选择目录, 页面显示通信异常(偶现)
118803	缺陷	ver2.0.5.4a17_CentOS7.2 64 位: 打开所有开关后连接代理端时 server 进程异常退出(出现一次)
118712	缺陷	ver2.0.5.4a17: web 端修改代理端通信接口后首次连接提示通信异常
118571	缺陷	ver2.0.5.4a17: 病毒查杀成功, 查杀列表数跟告警显示数目不一致, 隔离后搜索的数目跟查杀总数不一致
118569	缺陷	ver2.0.5.4a17: 代理端安装包目录下存在其他包含 rpm 字样的文件时安装不成功
118540	缺陷	ver2.0.5.4a17: 代理端进程重启后点击首页连接站点时提示通信异常
118527	缺陷	ver2.0.5.4a17 64 位_centos5.8: 打开安全主机开关内所有开关, 放置一天, 代理端 watchdog 和 server 文件大小发生变化, 不能手动执行
118512	缺陷	ver2.0.5.4a17_redhat6.5: 反弹 shell, socat 方式拦截, 代理端服务异常退出
118473	缺陷	ver2.0.5.4a17: 病毒扫描自定义扫描路径选择长路径, 扫描时代理端服务退出
118460	缺陷	ver2.0.5.4a17_CentOS7.9 64 位: 【程序白名单】取消扫描后, web 界面一直处于查询数据状态
118388	缺陷	ver2.0.5.4a17_CentOS7.2 64 位: 删除目录白名单过程中卸载内核再开启内核时代理端异常退出
118365	缺陷	ver2.0.5.4a17_CentOS7.9 64 位: 反弹 shell 开关为 ON, ruby 反弹 shell 攻击拦截失败
118363	缺陷	ver.0.5.4a17_CentOS7.9 64 位: 反弹 shell 开关为 ON, 使用 php 和

		lua 方式进行反弹 shell 攻击拦截时代理端服务异常退出
118362	缺陷	ver2.0.5.4a17: 反弹 shell 开关为 ON, wget 下载被杀死
118332	缺陷	ver2.0.5.4a17_BcLinux7.4: 代理端服务异常退出重启后再次进入病毒扫描页面, 自动进行全盘查杀
118326	缺陷	ver2.0.5.4a17_BcLinux7.4: 打开所有开关后进行漏洞扫描、病毒查杀, 代理端服务异常退出
118322	缺陷	ver2.0.5.4a17_CentOS7.2 64 位: 批量操作安全开关后切换页面时代理端概率异常退出
118241	缺陷	ver2.0.5.4a17: 病毒查杀隔离操作导致通信异常, 代理端服务重启
118233	缺陷	ver2.0.5.4a17_CentOS7.9 64 位: 防暴力破解 (非 OFF 状态) —— telnet 方式暴力破解达到次数不告警, web 界面也不产生规则
118220	缺陷	ver2.0.5.4a17: webshell 扫描成功, 再次连接站点, 提示通信异常
118200	缺陷	ver2.0.5.4a17: webshell 扫描, 扫描过程中重新登录并选择其他扫描路径, 提示匹配失败
118183	缺陷	ver2.0.5.4a17: license 过期, 采集许可证信息页面获取不到站点
118168	缺陷	ver2.0.5.4a17_redhat5.6-程序白名单: 扫描后取消, 操作很快, 报: 通信异常, 代理端
118146	缺陷	ver2.0.5.4a17_bcLinux7.4: 反弹 shell 开关为 ON 或 Warning 时拦截后代理端服务异常退出, 产生 core 文件
118145	缺陷	ver2.0.5.4a17: 关闭防火墙后查看防暴力破解规则, 管理端响应超时
118143	缺陷	ver2.0.5.4a17_redhat5.6-程序白名单: 添加文件白名单后扫描, 一直扫描中
118142	缺陷	ver2.0.5.4a17_redhat5.6-程序白名单: 添加文件白名单后扫描, 报通信异常
118138	缺陷	ver2.0.5.4a17_CentOS7.4&&Redhat5.8: 执行稳定性, ListenHostServer 和 ListenHostWatchDog 不停的重启
118134	缺陷	ver2.0.5.4a17: 非法 IP 白名单在非法时间段登录未产生告警
118111	缺陷	ver2.0.5.4a17: 白名单操作过程中手动卸载安全模块后 web 页面提示异常等问题
118096	缺陷	ver2.0.5.4a17_redhat6.5: 程序白名单-添加目录白名单, 下发过程中打开登录页面, 代理端服务异常退出
118059	缺陷	ver2.0.5.4a17: IPV6 站点新建 IPV4 防暴力破解限制规则时管理端响

		应超时
117823	缺陷	ver2.0.5.4a15_CentOS7.6 64 位: 恶意代码查杀《全盘查杀》快速查杀, 点击后, 执行一晚上, 仍处于查杀中
117692	缺陷	ver2.0.5.4a15_redhat5.6 64 位: 点击管理各界面, 各页面大概率刷不出来, 且频繁出现管理端 web 页面崩溃, 通信异常, 代理端服务重启现象
117672	缺陷	ver2.0.5.4a15_Redhat5.8 64 位 : 打开 DDOS 开关后进入 ddos 攻击防御页面, 提示“单个访问者并发链接数、服务器可承载总访问量、单个访问者总访问频率, 查询失败!”, 再连接站点没有响应(偶现)
117525	缺陷	ver2.0.5.4a15_redhat5.6 64 位: 重启主机后, 代理端显示过期
117374	缺陷	ver2.0.5.4a15_redhat7.3: 病毒查杀, 打开所有开关, 点击快速查杀, 代理端服务异常退出
117329	缺陷	ver2.0.5.4a15_Redhat5.8 实体机: 执行稳定性 3 天左右, 机器重启
117226	缺陷	ver2.0.5.4a15_redhat7.3: telnet 反弹 shell 引起代理端服务异常退出
117158	缺陷	ver2.0.5.4a15: 页面新建主机用户时代理端服务异常退出, 产生 core 文件
117131	缺陷	ver2.0.5.4a15_bclinux7.4: 进入病毒查杀页面后就自动进行全盘查杀, 并提示“全盘查杀失败!”, 且管理端服务异常退出
117127	缺陷	ver2.0.5.4a15: IPV6 修改防暴力破解规则为内核 IP 黑名单限制和可信成功
117008	缺陷	ver2.0.5.4a15: 内核开关和防火墙服务都关闭时, 点击防暴力破解配置失败
116995	缺陷	ver2.0.5.4a15_redhat7.4 (实体机): 程序白名单取消扫描提示成功实则未成功
116989	缺陷	ver2.0.5.4a15_redhat7.4 (实体机): 程序白名单取消扫描后 4611 端口被 ls 占用
116937	缺陷	ver2.0.5.4a15: 防暴力破解开关为 ON 时, 达到限制次数产生的规则为防火墙和内核黑名单限制
116935	缺陷	ver2.0.5.4a15: 已有防火墙和内核黑名单限制的规则时设置防暴力破解开关为 Warning 成功
116862	缺陷	ver2.0.5.4a15: 安装完代理端之后/usr/local/bin/uxsino 下存在占用大磁盘空间的文件

116825	缺陷	ver2.0.5.4a15_bcLinux7.4&&Redhat6.9:打开白名单开关后闲置一段时间,虚拟机卡住,通信异常
116307	缺陷	ver2.0.5.4a13_redhat5.6 64位:系统自带mysql数据库mysql-5.0.77工具可以成功连接,CDPS管理端的弱口令检测不能成功连接
116220	缺陷	ver2.0.5.4a13:IPV6点击安全文件检查后代理端服务异常退出,产生core文件
116205	缺陷	ver2.0.5.4a13_redhat6.5_64位:操作安全基线后,打开主机管理用户列表,概率出现代理端服务异常,显示通信异常
116181	缺陷	ver2.0.5.4a13_redhat6.5_64位:mysql基线选中全部加固,mysql服务启动失败
116119	缺陷	ver2.0.5.4a13:系统每产生任意一个告警就会产生一个僵尸进程
116111	缺陷	ver2.0.5.4a13_CentOS7.2 64位:使用python和java方式进行反弹shell攻击拦截时代理端服务异常退出
116105	缺陷	ver2.0.5.4a13:Java脚本、netcat、socat、awk、telnet工具反弹shell功能失效
116094	缺陷	ver2.0.5.4a13_CentOS7.2 64位:添加包含10w+文件目录白名单过程中代理端异常退出
116054	缺陷	ver2.0.5.4a13:打开所有开关后使代理端过期,代理端服务异常退出
116042	缺陷	ver2.0.5.4a13_Centos7.9:程序白名单添加超1k个文件的目录白名单时,前端页面一直显示下发中,实际所有文件已添加为白名单
116020	缺陷	ver2.0.5.4a13:将CPU休眠功能打开设置90%休眠,模板管理下发默认linux安全基线至Redhat5.9和centos6.4,都推送失败
115955	缺陷	ver2.0.5.4a13:防暴力破解相关操作产生僵尸进程
115954	缺陷	ver2.0.5.4a13:打开关闭所有开关都会产生一个僵尸进程
115940	缺陷	ver2.0.5.4a13:IPV6无法阻断反弹shell攻击
115907	缺陷	ver2.0.5.4a13:防暴力破解新建ipv6的规则后通信异常
115892	缺陷	ver2.0.5.4a13_Centos7.9:代理端安装完成后再设置系统白名单,白名单开关打开出现执行系统命令提示无权限,通信异常等问题
115873	缺陷	ver2.0.5.4a13_Centos7.9:程序白名单扫描时切换页面,扫描中断
115853	缺陷	ver2.0.5.4a13_Centos7.9:程序白名单扫描页面扫描过超10w个文件后,再次进入该页面显示正常查询数据超30分钟,导致无法进行

		白名单操作
115843	缺陷	ver2.0.5.4a13: 端口一键丢弃时 5005 也被丢弃
115627	缺陷	ver2.0.5.4a13: 反弹 shell 被阻断前短暂获取到靶机的 shell
115449	缺陷	ver2.0.5.4a13 64 位_redhat6.5: 开启防病毒及防暴力破解, 配置防暴力破解概率出现 popup 进程异常退出
115401	缺陷	ver2.0.5.4a13_CentOS7.9: 病毒查杀点击终止操作, 代理端主机异常, 且进程仍存在
115399	缺陷	ver2.0.5.4a13_CentOS6.4: 代理端有病毒文件时, 快速查杀和全盘查杀成功后都没有查出病毒
115393	缺陷	ver2.0.5.4a13_CentOS6.4: 自定义查杀病毒时查杀失败, 路径都正确的情况下提示路径不存在
115334	缺陷	ver2.0.5.4a13_CentOS7.9: 反弹 shell, 代理端攻击靶机后, 代理端服务异常
115329	缺陷	ver2.0.5.4a13_CentOS7.2 64 位: 反弹 shell 开关开启情况下代理端进程异常退出
115327	缺陷	ver2.0.5.4a13_CentOS5.8&&Redhat6.9: 反弹 shell 功能失效
115325	缺陷	ver2.0.5.4a13: 反弹 shell 白名单功能不生效
115323	缺陷	ver2.0.5.4a13: 每次拦截反弹 shell 后均产生一个 sh 的僵尸进程
115322	缺陷	ver2.0.5.4a13_redhat6.5_64 位: 特定环境下点击站点提示通信异常
115299	缺陷	ver2.0.5.4a13_CentOS6.4: 清除长路径下的文件时代理端服务重启通信异常
115277	缺陷	ver2.0.5.4a13_CentOS7.2 64 位: license 过期或者过期恢复时代理端异常退出
115270	缺陷	ver2.0.5.4a13_CentOS7.9: 系统, 中间件, 数据库基线模板下发失败
115268	缺陷	ver2.0.5.4a13 64 位_CentOS7.9: 执行稳定性过程中 license 授权过期
115249	缺陷	ver2.0.5.4a13_CentOS7.9: 内核加载开关打开, 代理端重启后显示安全内核开关关闭
115141	缺陷	ver2.0.5.4a13_CentOS7.4: 稳定性环境按步骤设置后通信异常
114068	缺陷	ver2.0.5.4a11_redhat7.2: 白名单扫描页面, 点击路径框, 提示查询扫描状态失败
113823	缺陷	ver2.0.5.4a11 64 位_redhat6.5: 防病毒扫描取消之前隔离文件, 重

		新进行扫描，扫描病毒个数与初始个数存在不一致情况（偶现）
113809	缺陷	ver2.0.5.4a11_IPV6_中国移动 bclinux: ipv6 产生防暴力破解告警后点击防暴力破解页面代理端服务挂掉
113800	缺陷	ver2.0.5.4a11 64 位_redhat6.5: 防病毒扫描选择模式二，代理端进程异常，有 core 文件
113775	缺陷	ver2.0.5.4a11 64 位_redhat6.5: 防暴力破解开关关闭后，拦截依旧生效
113729	缺陷	ver2.0.5.4a11_中国移动 bcLinux7.4: 下发文件完整性检查模板时代理端服务异常退出，通信异常
113701	缺陷	ver2.0.5.4a11_redhat7.2: 普通用户远程 ssh 登录，su 到 root，安装代理端后会产生大量的审计日志
113688	缺陷	ver2.0.5.4a11_redhat7.2: 日志备份管理，鉴别日志备份设置 10M，但日志产生备份时大小超过了 10M
113668	缺陷	ver2.0.5.4a11_Centos5.7 64 位: 打开内核和白名单开关后，再次连接站点访问超时后报通信异常
113656	缺陷	ver2.0.5.4a11_redhat7.2: 普通用户远程登录 su 到 root 安装 cdps 代理端，服务基本 10 分钟左右挂一次
113615	缺陷	ver2.0.5.4a11 64 位_Centos7.8: 卸载代理端后，重新安装代理端，4611 端口被 rpcbind 占用
113544	缺陷	ver2.0.5.4a10 64 位_Centos7.9: 稳定性测试中持续执行白名单脚本，授权期限变为 0 天，license 文件大小为 0
113540	缺陷	ver2.0.5.4a11_Redhat5.9: ListenHostServer 执行重启后自动离线，4611 端口被自动释放
113516	缺陷	ver2.0.5.4a11:Redhat5.9 和 Centos6.4 同时在线时文件完整性检查模板 Redhat5.9 下发不能完成,Redhat5.9 ListenHostServer 重启
113474	缺陷	ver2.0.5.4a11_Centos7.9: oracle 基线模板下发失败
113417	缺陷	ver2.0.5.4a11_Rehat5.9: web 执行程序白名单的+, ListenHostServer 会重启，白名单初始化失败
113394	缺陷	ver2.0.5.4a11_CentOS7.2 64 位: 取消扫描后再次扫描等问题
113353	缺陷	ver2.0.5.4a11_linux5&linux6: 执行 SU 拦截、强访拦截后代理端服务异常退出
113344	缺陷	ver2.0.5.4a11_linux5&linux6: 执行白名单拦截后代理端服务重启，通信异常

113329	缺陷	ver2.0.5.4a11_CentOS6.4 64 位：安装代理端时系统一直没有完成
113292	缺陷	ver2.0.5.4a11 64 位_Centos7.8：安装部署代理端失败
112982	缺陷	ver2.0.5.4a10_Rehat5.9：正在进行选择文件升级弱口令特征库，突然弹窗一个窗口提示获取数据失败，然后 web 连不上了
112962	缺陷	ver2.0.5.4a10_Centos5.7 64 位系统测试：centos5.7 系统没有启用 ipv6 时管理端安装失败
112953	缺陷	ver2.0.5.4a10_Centos5.7 64 位系统测试：首页显示有误
112952	缺陷	ver2.0.5.4a10_CentOS7.2 64 位:ListenHostServer 正常运行中 4611 端口被 popup 占用
112927	缺陷	ver2.0.5.4a10：web 页面批量下发时不显示 linux 站点（偶现）
112896	缺陷	ver2.0.5.4a10 64 位_Centos7.8：白名单扫描线程数配置未做限制，当为负数时，扫描结果为空
112891	缺陷	ver2.0.5.4a10_CentOS7.2 64 位：popup 占用 4611 端口导致 ListenHostServer 进程无法启动（偶现）
112890	缺陷	ver2.0.5.4a10 RedHat/CentOS 7 的系统 64 位：模板管理-文件完整性模板，创建空的完整性模块并添加自定义文件完整性路径例如:/var/log/*下发后，病毒查杀、清除文件信息、白名单扫描等列表内容无法加载
112849	缺陷	ver2.0.5.4a10_Rehat6.9：长路径文件添加目录白名单时代理端服务退出，通信异常
112841	缺陷	ver2.0.5.4a10_Redhat6.9：白名单拦截长度 510 的文件后，点击 popup 异常退出
112821	缺陷	ver2.0.5.4a10_Rehat6.8：自定义查杀病毒后 4611 端口被占用，web 通信异常
112807	缺陷	ver2.0.5.4a10：代理端主机过期后重启主机再恢复授权开关状态问题
112784	缺陷	ver20.5.4a10_CentOS7.2 64 位：代理端过期后重启代理端主机内核自动加载及远程登录开关打开
112779	缺陷	ver2.0.5.4a10_Centos5.7 64 位系统测试：文件管理》白名单扫描，点击删除文件白名单按钮下发时提示通信异常
112775	缺陷	ver2.0.5.4a10：添加或删除目录白名单选择不操作子目录时不生效
112770	缺陷	ver2.0.5.4a10_Redhat6.9：取消扫描白名单时，页面卡死，再次进入时通信异常

112589	缺陷	ver2.0.5.4a10_Rehat5.9: 代理端为 IPV6 时 web 链接站点通信异常
112556	缺陷	ver2.0.5.4a10: 已添加白名单的文件后, 再创建一个内容相同的文件, 未识别为白名单文件
112554	缺陷	ver2.0.5.4a10_中国移动: 管理端用 ipv6 打开的 web 界面许可证管理界面未获取到管理端和代理端的许可证
112542	缺陷	ver2.0.5.4a10: 白名单扫描页面全部选中 10w 个文件点击删除文件白名单时提示失败
112530	缺陷	ver2.0.5.4a10_CentOS7.2 64 位: 文件列表查询提示失败且进入到其他页面代理端进程异常退出
112482	缺陷	ver2.0.5.4a10: 批量添加目录白名单时管理端心跳处理异常
112481	缺陷	ver2.0.5.4a10_Centos7.9: uxdb 基线, 目前.uxpass 的写入方式导致执行基线脚本时需要输入用户口令, 修改.uxpass 文件的写入方式
112478	缺陷	ver2.0.5.4a10: 白名单扫描过程中取消失败等问题
112468	缺陷	ver2.0.5.4a10: 同时下发 2 台虚拟机的白名单添加, 一台虚拟机没有该路径时任务不能自动结束, 会通信异常
112389	缺陷	ver2.0.5.4a10_Rehat6.9: 长路径目录白名单扫描代理端服务退出, 通信异常
112388	缺陷	ver2.0.5.4a10_Rehat5.9: kill 了 watchdog 相关的两个进程后 ListenHostServer 进程也不见了
112384	缺陷	ver2.0.5.4a10 CentOS 7.7 64 位: 报警工作站-程序白名单历史告警, 分页组件点击下一页按钮报通信异常, 多个系统必现
112350	缺陷	ver2.0.5.4a10_Rehat5.9: 漏洞扫描完成系统安全员超时再次登录系统提示通信异常
112345	缺陷	ver2.0.5.4a10: 长文件进入路径第一次提示“文件目录名过长, 显示该目录失败!”, 再次点击通信异常
112344	缺陷	ver2.0.5.4a10_Rehat5.9: 漏洞扫描完成后第二次进入页面没有漏扫结果, 显示的是未进行漏洞扫描, 通信异常
112341	缺陷	ver2.0.5.4a10: 较长路径 webshell 文件隔离、扫描失败且代理端服务退出
112333	缺陷	ver2.0.5.4a10 Red Hat6 和 Red Hat7: 文件管理-白名单扫描, 无法对有特殊字符的目录和根目录添加白名单
112329	缺陷	ver2.0.5.4a10 Red Hat 5.8 实体机 64 位: 代理端安装完毕, ListenHostServer 不停重启, 严重影响用户正常使用

112326	缺陷	ver2.0.5.4a10 CentOS 7.7 64 位：文件管理-白名单扫描，在白名单扫描页面对根路径下的目录进行操作后，再次进入白名单扫描等页面提示查询失败，必现
112291	缺陷	ver2.0.5.4a10_Redhat6.9：文件列表没有添加白名单和删除白名单
112271	缺陷	ver2.0.5.4a10_Redhat6.9：白名单告警添加信任时将根目录下所有文件都添加了白名单，新建文件也自动加入白名单
112263	缺陷	ver2.0.5.4a10：远程登录开关开启后普通用户无法桌面登录
112064	缺陷	ver2.0.5.4a6 64 位_Redhat6.9：使用 icmp flood 或者 udp flood 进行攻击，代理端挂掉，页面通信异常
112062	缺陷	ver2.0.5.4a6_Redhat6.9：下发安全基线模板后过期及恢复，部分加固项状态有变化
112058	缺陷	ver2.0.5.4a6_Redhat6.9：默认安全基线过期后及恢复后，部分加固项状态有变化
112006	缺陷	ver2.0.5.4a6_Rehat5.9：打开一些开关后查询系统信息失败
111965	缺陷	ver2.0.5.4a6_CentOS7.7：ListenHostServer 掉线后，WatchDog 无法拉起，快照必现
111747	缺陷	ver2.0.5.4a6 RedHat7.6 64 位：主机安全开关-安全内核，代理端安装完毕第一次下发安全内核开关后，点击站点信息通信异常，必现
111731	缺陷	ver2.0.5.4a6_Centos7.9:mysql 基线加固-多项加固完成状态依然显示不符合
111724	缺陷	ver2.0.5.4a6_Centos7.9：mysql 基线，加固后重新加固，web 页面卡住
111709	缺陷	ver2.0.5.4a6 CentOS7.7 64 位：主机安全开关-硬盘阈值，设置告警时间为 0 时 2 分，通信异常无法进入站点内部，快照必现
111684	缺陷	ver2.0.5.4a6 64 位_Centos7.9：用户权限管理页面显示为空，数据表查询为空
111670	缺陷	ver2.0.5.4a6_Redhat6.9：漏洞扫描失败
111599	缺陷	ver2.0.5.4a6_Rehat7.4：实体机稳定性环境执行到将 root 设置为 so 6 时发生了 error，稳定性无法执行
111576	缺陷	ver2.0.5.4a6 CentOS7.7 64 位：使用 IPV6 模式安装，完成安装后点击 IPV6 站点通信异常，无法进入站点内部
111573	缺陷	ver2.0.5.4a6_Centos7.9：代理端开启防火墙，web 页面查看提示：防火墙服务未开启

111563	缺陷	ver2.0.5.4a6 64 位_Centos7.8: 防火墙服务启动失败
111548	缺陷	ver2.0.5.4a6 64 位_Centos7.8: DDOS 攻击防护开关下发失败
111540	缺陷	ver2.0.5.4a6: 下发安全开关失败, 提示获取开关状态失败
110350	缺陷	ver2.0.5.4a5_Redhat7.6: 勾选全部 mysql 安全基线加固时代理端异常重启
109371	缺陷	ver2.0.5.4a5_Redhat7.6: 执行代理端卸载脚本, 机器重启
109102	缺陷	ver2.0.5.4a5: 批量修改超过 4 个告警等级后, 报通信异常, 且 ListenhostServer 无法被拉起
108939	缺陷	ver2.0.5.4a5_Redhat6.9: 第一次新建自定义模板时会出现数据库异常提示
107863	缺陷	ver2.0.5.4a5:CDPS 正常使用后闲置一段时间后再次登录提示通信异常
107834	缺陷	ver2.0.5.4a5_Redhat6.9: 给中间件自定义 NGINX 模板增加加固项时提示“数据库异常”
107832	缺陷	ver2.0.5.4a5_Redhat6.9: 新建中间件自定义模板时提示“添加中间件安全基线 Apache_Tomcat 基线模板数据异常!”
107495	缺陷	ver2.0.5.4a5_CentOS7.4 : 代理端安装完成后 watchdog 无法启动成功等问题
107414	缺陷	ver2.0.5.4a5 RedHat7.6 64 位: 漏洞扫描完毕后, 从首页点击站点拓扑, 多次尝试都为黑屏并报通信异常, 无法进入
107410	缺陷	ver2.0.5.4a5 64 位: 配置 22 端口导致系统无法访问
107347	缺陷	ver2.0.5.4a5_Redhat6.9 64 位: 告警等级批量下发时代理端服务退出且不能被拉起
107346	缺陷	ver2.0.5.4a5_Redhat5.8 64 位: 资源管理中主机用户弱口令字典上传后没有任何文件, 不能进行弱口令字典升级
107278	缺陷	ver2.0.5.4a5 RedHat7.6 64 位: 打开内核开关, 机器重启
107269	缺陷	ver2.0.5.4a5_Redhat5.8 64 位: 打开安全模块和一些开关后, 链接站点, 通信异常
107267	缺陷	ver2.0.5.4a5: 较长路径的 webshell 文件扫描后隔离、信任、下载操作都失败
107264	缺陷	ver2.0.5.4a5 RedHat7.6 64 位: ListenHostServer 掉线后, 没法拉起来
107234	缺陷	ver2.0.5.4a5_CentOS7.4 64 位: 稳定性环境链接站点后通信异常,

		web 无法正常使用
107233	缺陷	ver2.0.5.4a5_Redhat5.8 64 位：打开安全开关后代理端不能打开终端
107155	缺陷	ver2.0.5.4a5_Redhat6.9 64 位：安装后点击安全文件检查，通信异常，代理端服务重启
107151	缺陷	ver2.0.5.4a5_Redhat6.9 64 位：点击 webshell 后门检测后，页面提示通信异常，代理端服务未重启(偶现)
100629	缺陷	ver2.0.5.4a4_Centos7.4: license 恢复后收到过期时操作产生的告警
100616	缺陷	ver2.0.5.4a4_Centos7.4: license 过期后，非法 IP/账号检测仍然生效
100580	缺陷	ver2.0.5.4a4_Centos7.4: license 过期并恢复后，命令行防御规则失效
100571	缺陷	ver2.0.5.4a4_Centos7.4: 命令行防御新建进程名包含路径，防御失效
99659	缺陷	ver2.0.5.4a3_Redhat6.8: 命令防御添加删除都没有记录 linux 鉴别日志
99633	缺陷	ver2.0.5.4a3_RedHat5.9 64 位：攻击防御-命令行防御，添加任意一条命令会对其他命令造成影响，对 iptables 造成影响时可能无法访问 WEB 页面
99528	缺陷	ver2.0.5.4a3 64 位：webshell 文件较大时，批量信任信任失败
99405	缺陷	ver2.0.5.4a3_Redhat6.8: 病毒隔离开关打开，自定义查杀病毒时 CPU 超高，ListenHostServer 服务重启
99368	缺陷	ver2.0.5.4a3_Redhat6.8: 病毒查杀结果为空，查杀结束后点击页面提示防病毒开关查询失败， ListenHostServer 服务不在线
98758	缺陷	ver2.0.5.4a2_Redhat6.4 64 位：新建端口防火墙规则后点击一键丢弃和一键接受，一个端口变成了多条规则
98741	缺陷	ver2.0.5.4a2_Centos7.2: 代理端服务重启后，弱口令字典数据重复
98732	缺陷	ver2.0.5.4a2_CentOS6.5: webshell 后门检测扫描不出来 webshell 文件
98612	缺陷	ver2.0.5.4a2_Centos6.5 64 位：弱口令字典升级后 web 看到的弱口令字典条数与原来有差异
98608	缺陷	ver2.0.5.4a2_Centos6.5 64 位：弱口令字典升级失败

98576	缺陷	ver2.0.5.4a2_CentOS7: 安全基线加固时出现一个代理端服务同名的子进程
98489	缺陷	ver2.0.5.4a2_CentOS7.6: 强访规则的 mv 和 rm 功能失效
98488	缺陷	ver2.0.5.4a2_CentOS7.6: 一个文件出现了三条强访规则
98453	缺陷	ver2.0.5.4a2_CentOS7.2: SU 拦截成功但未产生告警
98326	缺陷	ver2.0.5.4a2_CentOS6.5 64 位: 防火墙开启的情况下新建防暴力破解不成功, 提示防火墙没开启
98323	缺陷	ver2.0.5.4a2_CentOS5.9 64 位 : 资源管理-设备发现, 在 Linux5 老系统中, 通过 IPV4 和 IPV6 格式无法发现设备
98212	缺陷	ver2.0.5.4a2_CentOS7.6 64 位: 实体机上打开反弹 shell 开关, ListenHostServer 不停重启, CPU 达到 98%
98162	缺陷	ver2.0.5.4a2_CentOS7.2: webshell 隔离文件失败
98155	缺陷	ver2.0.5.4a2_CentOS7.2: 病毒扫描模式一扫描不到病毒
98137	缺陷	ver2.0.5.4a2_CentOS6.5 64 位: 一部分隔离的病毒添加信任失败, 取消隔离也失败
98123	缺陷	ver2.0.5.4a2_CentOS6.5 64 位: 病毒隔离开关打开查杀出的病毒仍然有很多病毒隔离失败, 处于未处理状态
98119	缺陷	ver2.0.5.4a2_CentOS6.5 64 位: 一部分隔离的病毒不能被清除
98066	缺陷	ver2.0.5.4a2_CentOS7.2: 同时打开所有开关, 代理端服务重启, 站点离线
97947	缺陷	ver2.0.5.4a2_CentOS5.9 64 位 : 开启安全内核和命令行防护开关, 在 CentOS5.9 系统中无法打开 shell 窗口
97011	缺陷	ver2.0.5.4a1_redhat7.2 64 位: 安全基线加固项列表为空
96940	缺陷	ver2.0.5.4a1_redhat7.5: 模板下发后, 安全基线的描述中出现部分前端代码
96903	缺陷	ver2.0.5.4a1_redhat7.5: 下发模板后, 连接站点查看加固项名称和描述有误
96857	缺陷	ver2.0.5.4a1: webshell 检测, 输入根目录扫描提示扫描失败
96803	缺陷	ver2.0.5.4a1_redhat7.5: webshell 检测路径配置含有通配符时, 代理端服务重启
96717	缺陷	ver2.0.5.4a1_redhat7.2 64 位: 用户配置了公钥 key, 且能使用该公钥登录成功, 但 web 界面用户公钥 key 仍显示 never
96658	缺陷	ver2.0.5.4a1_redhat7.5: 永久授权后系统过期等问题

96647	缺陷	ver2.0.5.4a1_redhat7.6 64 位: 跑稳定性脚本代理端服务总是重启, top 查看 CPU 占有率一直在 98%
96614	缺陷	ver2.0.5.4a1_redhat7.6 64 位: 审计状态开启时默认审计规则不能显示
96603	缺陷	ver2.0.5.4a1_RedHat6.2 64 位 :主机安全开关,在 IPV6 通信模式下,开启非法外联等开关,主机内部无法访问 web 页面
96512	缺陷	ver2.0.5.4a1_redhat5.4 64 位: 重启 ListenHostServer 服务后 ListenHostWatchDog 进程不见了
96502	缺陷	ver2.0.5.4a1_Redhat7.6 64 位: 弱口令告警没有上报告警中心
96423	缺陷	ver2.0.5.4a1_redhat7.5: 防暴力破解开关 WARNING 时, 35 和 37 未进行攻击但产生了防暴力破解告警且加入了规则列表
96342	缺陷	ver2.0.5.4a1_redhat7.5: 防暴力破解开关 ON 时 35 和 37 未进行攻击但产生了防暴力破解告警
96250	缺陷	ver2.0.5.4a1_redhat7.5: 设置 CPU/MEM 阈值休眠后, CPU 和内存占用率超过阈值后, 代理端服务仍能被 watchdog 拉起
96234	缺陷	ver2.0.5.4a1 : 自定义查杀失败 总是提示路径不存在
96232	缺陷	ver2.0.5.4a1: 快速查杀结果为空

4 参考文档

序号	参考文档	说明
1.	用户手册	参见优炫操作系统安全增强系统 (CDPS) V5.4.docx
2.	测试报告	参见优炫操作系统安全增强系统 (web 版) 用户手册_5.4.docx
3.	技术白皮书	参见技术白皮书.docx
4.	安装卸载文档	参见 CDPS2.0.5.4 安装手册.docx
5.	销售一指禅	参见 CDPS 销售一指禅 v1.0.docx