编号	1
日期	2024-08-14

openkylin本地安全检测报告

■ 版权声明

本地安全漏洞检测工具为本团队编写。

■ 适用声明

本地安全漏洞检测工具可用于测试Linux系操作系统中是否存在可利用的中　高风险漏洞。本工具支持通过原理扫描发现漏洞、支持通过版本匹配的方式 发现CVE漏洞以及支持安全基线检测。

■ 免责声明

本报告为本工具根据使用者检测结果自动生成的报告，报告内容不代表本团队的立场及观点。由于传播、利用此工具提供的检测功能而造成的任何直接或者间接的后果及损失，均由使用者本人负责，本团队不为此承担任何责任。

■ 开发团队

以下贡献者排名不分先后： 刘鑫、乔嘉琛、谢幸

一、报告摘要

被扫描平台： 192.168.160.133

表1 目标信息

用户名	liuxin
计算机名	nucKylin
操作系统名	NAME="优麒麟"
操作系统版本	ubuntukylin-22.04-pro
系统架构	amd64
内核版本	linux 5.15.0-107-generic

任务模式：原理扫描

表 2 扫描任务信息

加载数	115个
发起扫描时间	18:15:00
扫描完成时间	18:21:39
危险基线数	0个
发现漏洞数	5个
漏洞级别分布	高危0个 中危2个 低危3个

未执行成功表:

表3 未执行表

系统未执行数	0
内核未执行数	0
安全基线未执行数	0

二. 基线扫描列表

表4 基线列表

索引	所属	站点信息名称	修复结果
1	2账号口令	检查是否以设置口令生存周期	安全
2	2账号口令	检查设备密码复杂度策略	安全
3	2账号口令	检查是否存在空口令账户	安全
4	2账号口令	检查是否设置口令最小长度	安全
5	4日志审计	检查是否配置远程日志功能	应对远程日至进行筛选与审核。此检查项建议调整
6	2账号口令	检查是否设置除root之外UID为0的用户	安全
7	3认证授权	检查/etc/shadow文件权限	安全
8	3认证授权	检查/etc/bashrc文件中umask设置	安全
9	5协议安全	检查使用ip协议远程维护的设备是否配置ssh协议，禁用telnet协议	Telnet协议名文传输，安全性低，容易被嗅探泄漏信息。此检查项建议调整手动调整

三. 漏洞详情

表5 系统漏洞检测详情

索引	1
CVE-ID	CVE-2022-2639
危害等级	高
发现时间	2022-09-01
漏洞详情	业界披露了Linux Kernel openvswitch模块权限提升漏洞（CVE-2022-2639）的漏洞细节。由于 openvswitch模块中reserve_sfa_size()函数在使用过程中存在缺陷，导致本地经过身份认证的攻击者可以利用漏洞提升至root权限。目前漏洞poc已公开，风险较高。
漏洞影响	1. 采用容器隧道网络的CCE集群，节点OS镜像使用了EulerOS 2.8（ARM场景）或EulerOS 2.9。 2. 节点OS镜像使用了Ubuntu。
修复方案	容器内进程使用非root用户启动的进程可以通过为工作负载配置安全计算模式seccomp，建议配置imeDefault模式或者禁用unshare等系统调用。具体配置方法可参考社区官方资料使用 Seccomp 限制容器的系统调用。 1.Ubuntu镜像自带openvswitch内核模块，可以通过将禁止加载openvswitch 内核模块来规避。操作如下： echo "blacklist openvswitch" >>/etc/modprobe.d/blacklist.conf

索引	2
CVE-ID	CVE-2022-0185
危害等级	高
发现时间	2022-01-27
漏洞详情	国外安全研究人员William Liu和Jamie Hill-Daniel发现Linux内核中包含一个整数溢出漏洞，可导致写操作越界。本地攻击者可以使用这一点导致拒绝服务(系统崩溃)或执行任意代码，在容器场景下拥有CAP_SYS_ADMIN权限的用户可导致容器逃逸到宿主机。目前已存在poc，但尚未发现已公开的利用代码。
漏洞影响	容器内用户拥有CAP_SYS_ADMIN权限，并且内核版本在5.1以及以上。在标准的docker环境下，由于使用了Docker seccomp filter，默认情况下不受该漏洞影响。在Kubernetes场景下，默认禁用了seccomp filter，在内核以及权限满足时受该漏洞影响。
修复方案	判断方法 uname -a查看内核版本号 规避和消减措施 CCE集群节点不受该漏洞影响。对于自建的K8s集群，建议用户对工作负载： 最小权限运行容器 根据社区提供的配置方法配置seccomp

索引	3
CVE-ID	CVE-2019-11477
危害等级	高
发现时间	2019-06-17
漏洞详情	2019年6月18日，Redhat发布安全公告，Linux内核处理器TCP SACK模块存在3个安全漏洞(CVE-2019-11477、CVE-2019-11478、CVE-2019-11479)，这些漏洞与最大分段大小（MSS）和TCP选择性确认（SACK）功能相关，攻击者可远程发送特殊构造的攻击包造成拒绝服务攻击，导致服务器不可用或崩溃。
漏洞影响	影响Linux内核2.6.29及以上版本。
修复方案	此问题已在稳定内核版本4.4.182、4.9.182、4.14.127、4.19.52、5.1.11中修复，用户通过滚动升级节点即可。

索引	4
CVE-ID	CVE-2023-52753
危害等级	高
发现时间	2023年
漏洞详情	此漏洞存在于Linux内核的drm/amd/display部分，涉及空指针解引用的问题。具体来说，是在访问定时生成器的函数之前，未检查分配的定时生成器是否为NULL，可能导致空指针解引用。
漏洞影响	攻击者可能利用此漏洞执行恶意代码或导致系统不稳定。
修复方案	及时更新Linux内核以修复此漏洞。

索引	5
CVE-ID	CVE-2023-52817
危害等级	高
发现时间	2022-01-27
漏洞详情	此漏洞影响Linux内核中的drm/amdgpu部分，当smcrreg指针为NULL时，可能导致异常的空指针访问。在特定类型的芯片上，如VEGA20，读取amdgpuregssmc文件时可能会触发此问题。
漏洞影响	攻击者可能利用此漏洞执行恶意代码或导致系统崩溃。
修复方案	应用官方发布的补丁或更新。