安全漏洞通告

CVE-2021-33909：Linux kernel 本地提权漏洞通告

360CERT

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-33909：Linux kernel 本地提权漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072202
报告版本	1	报告日期	2021-07-22
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-07-22	360CERT	360CERT	撰写报告

目录

360CERT

1 漏洞简述

2021 年 07 月 22 日，360CERT 监测发现 RedHat官方 发布了 Linuxkernel本地提权漏洞 的风险通告，漏洞编号为 CVE-2021-33909 ，漏洞等级：高危，漏洞评分：7.0。

该漏洞是Linuxkernel文件系统层的类型转换漏洞，类型转换漏洞是在两种类型之间进行转换时出现的一种情况，可能导致溢出。无特权的本地攻击者可以利用该漏洞进行权限提升。

对此，360CERT 建议广大用户及时将 Linux 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

360CERT

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	高危
影响面	广泛
攻击者价值	高
利用难度	高
360CERT 评分	7.0

360CERT

3 漏洞详情

3.1 CVE-2021-33909: Linux kernel 特权提升漏洞

CVE: CVE-2021-33909

组件: Linux kernel

漏洞类型: 特权提升

影响: 权限提升；服务器接管

简述: 在Linuxkernel文件系统层的seq_file.c文件中，由于没有正确地限制seq缓冲区的分配，未验证size_t-to-int的转换，导致整数溢出、越界写。无特权的本地攻击者可以通过创建、挂载和删除总路径长度超过 1GB 的深层目录结构来利用这个漏洞，该漏洞能够使无特权用户升级到root用户。

360CERT

4 影响版本

组件	影响版本	安全版本
Linux kernel	>=3.16 / <= 5.13.3	5.13.4

360CERT

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本。

具体升级请参考官方通告：

RedHat 官方通告

360CERT

6 时间线

2021-07-20 RedHat 发布通告

2021-07-22 360CERT 发布通告

360CERT

7 参考链接

RedHat 官方通告

linux github commit

360CERT

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或(shaoyulong#360.cn) 获取对应产品。

A.2 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元(探针）规则和本地安全大脑关联分析规则，做好防护。

A.3 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。