

安全漏洞通告

【POC 公开】 CVE-2021-36934: Windows 特权提升漏洞通告

报告信息

报告名称	【POC 公开】CVE-2021-36934: Windows 特权提升漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-072203
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

1	漏洞简述	3
2	风险等级	4
3	漏洞详情	5
	CVE-2021-36934: Windows 特权提升漏洞	5
4	影响版本	6
5	修复建议	7
	通用修补建议	7
6	时间线	8
7	参考链接	9
	附录	10
A	产品侧解决方案	10
	360 安全分析响应平台	10
	360 安全卫士	10
	360 本地安全大脑	11
	360 终端安全管理系统	11

1 漏洞简述

近日 360CERT 监测发现微软发布了Windows特权提升漏洞的风险通告，漏洞编号为 CVE-2021-36934，漏洞等级：严重，漏洞评分：7.8。

目前官方没有针对该漏洞的补丁，成功利用此漏洞的攻击者可以将普通用户权限提升至 SYSTEM 权限，并在目标机器上执行任意代码。对于攻击者的利用价值高。

该漏洞需要开启系统保护，并设置系统还原点才可利用，同时据官方描述该漏洞影响 Windows 10 1809 及之后的版本，具有一定的版本限制。但由于目前官方没有针对该漏洞的补丁，且在公网上存在已公开的漏洞利用程序，该漏洞的可利用性仍然极高。

对此，360CERT 建议广大用户参考修复建议及时进行临时防御。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。

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	严重
影响面	广泛
攻击者价值	高
利用难度	低
360CERT 评分	7.8

3 漏洞详情

3.1 CVE-2021-36934: Windows 特权提升漏洞

CVE: CVE-2021-36934

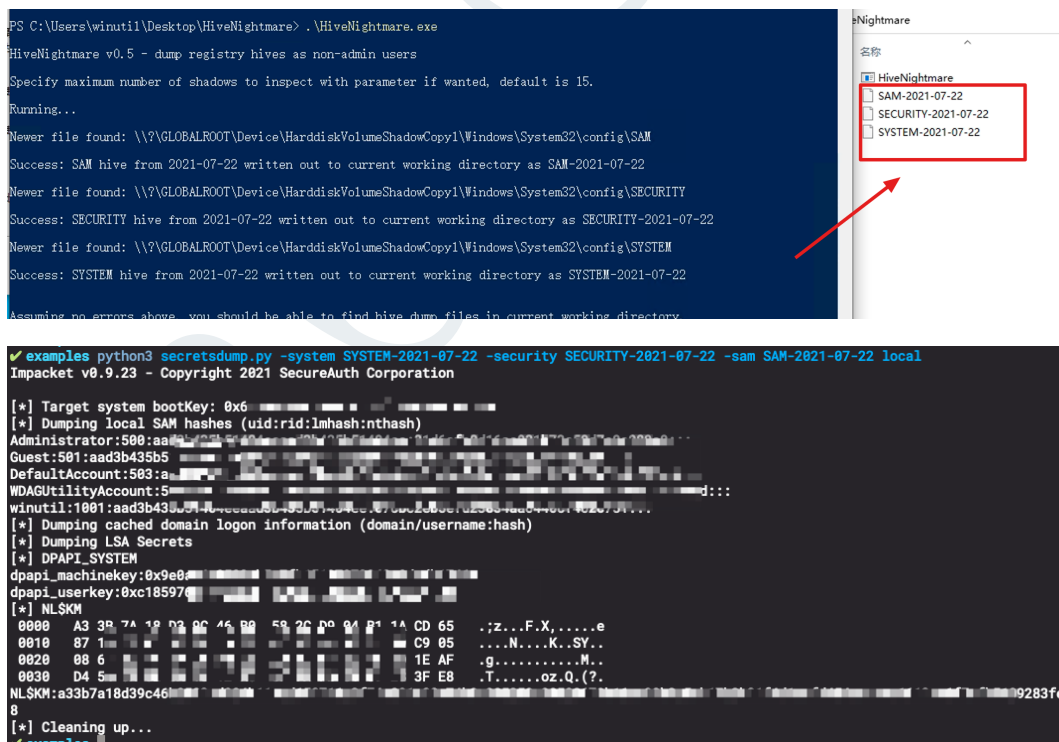
组件: Windows10

漏洞类型: 特权提升

影响: 特权提升

简述: 该漏洞是由于 Windows 对多个系统文件 (包括安全账户管理器 (SAM)) 的访问控制列表 (ACL) 过于宽松所导致的特权提升漏洞。成功利用此漏洞的攻击者可以将普通用户权限提升至 SYSTEM 权限, 并在目标机器上执行任意代码, 从而达到控制目标系统的目的。

该漏洞存在一定的前置利用条件，需要目标系统开启系统保护，并设置了系统还原点才可进行攻击。目前 360CERT 已经复现该漏洞：



4 影响版本

- Microsoft:Windows10: 1809 及之后的版本

5 修复建议

5.1 通用修补建议

目前该漏洞暂无官方补丁，官方推荐使用以下方式进行防御：

限制外部对%windir%\system32\config文件的访问：

1. 以管理员权限打开 CMD 或 PowerShell
2. 运行该命令：`icacls%windir%\system32\config\*/inheritance:e`

删除卷影复制服务（VSS）副本：

1. 删除限制访问%windir%\system32\config之前存在的所有系统还原点和卷影
2. 创建一个新的系统还原点

6 时间线

2021-07-20 微软发布通告

2021-07-21 360CERT 监测 POC 公开

2021-07-22 360CERT 完成 POC 验证并发布通告

7 参考链接

微软官方通告

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 安全卫士

Windows 用户可通过 360 安全卫士实现对应补丁安装、漏洞修复、恶意软件查杀，其他平台的用户可以根据修复建议列表中的安全建议进行安全维护。

360CERT 建议广大用户使用 360 安全卫士定期对设备进行安全检测，以做好资产自查以及防护工作。



A.3 360 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.4 360 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。

