安全漏洞通告

CVE-2021-36958: Windows Print Spooler 打印机漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-36958: Windows Print Spooler 打印机漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-081202
报告版本	1	报告日期	2021-08-12
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	2021-08-12	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-2021-36958: 代码执行漏洞 5
4 影响版本 6
5 修复建议 7
临时修补建议 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 本地安全大脑 10
360 终端安全管理系统 11

1 漏洞简述

2021 年 08 月 12 日，360CERT 监测发现 微软 发布了 PrintSpooler远程代码执行漏洞的风险通告，漏洞编号为 CVE-2021-36958 ，漏洞等级：严重，漏洞评分：9.9。

该漏洞与之前的 PrintNightmare 性质类似，目前尚无更多细节公开，且无漏洞补丁

微软官方标识该漏洞利用等级高

Windows Print Spooler 是用于管理打印机的后台服务，对于办公场景该服务是一定会被频繁使用，且持续在电脑中运行。这就给予了攻击者相应的攻击场景。

对此，360CERT 建议广大用户及时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	高
360CERT 评分	9.9

3 漏洞详情

3.1 CVE-2021-36958: 代码执行漏洞

CVE: CVE-2021-36958

组件: Windows Print Spooler

漏洞类型: 代码执行

影响: 服务器接管

4 影响版本

- Microsoft:Windows: [*]
- Microsoft:WindowsServer: [*]

5 修复建议

5.1 临时修补建议

若无域内打印机使用需求，可在域控制器，以及域内高权限服务器上禁用打印机服务。

```
Stop-Service -Name Spooler -Force

Set-Service -Name Spooler -StartupType Disabled
```

6 时间线

2021-08-11 微软发布安全通告

2021-08-12 360CERT 发布通告

7 参考链接

Windows Print Spooler Remote Code Execution Vulnerability

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。