CVE-2020-0796：微软 SMBv3 协议RCE检测

原创shiyi Timeline Sec
2020-03-14原文

收录于话题
#漏洞复现文章合集
70个

本公众号专注于最新漏洞复现，欢迎关注！

-

本文作者：shiyi（Timeline Sec复现组成员）
本文共684字，阅读大约需要2~3分钟
声明：请勿做非法用途，否则后果自负

0x01 简介

SMB(全称是Server Message Block)是一个协议名，它能被用于Web连接和客户端与服务器之间的信息沟通。

0x02 漏洞概述

该漏洞是由于SMBv3协议在处理恶意的压缩数据包时出错所造成的，它可让远程且未经身份验证的攻击者在目标系统上执行任意代码。该漏洞类似于永恒之蓝，存在被蠕虫化利用的可能。

0x03 影响版本

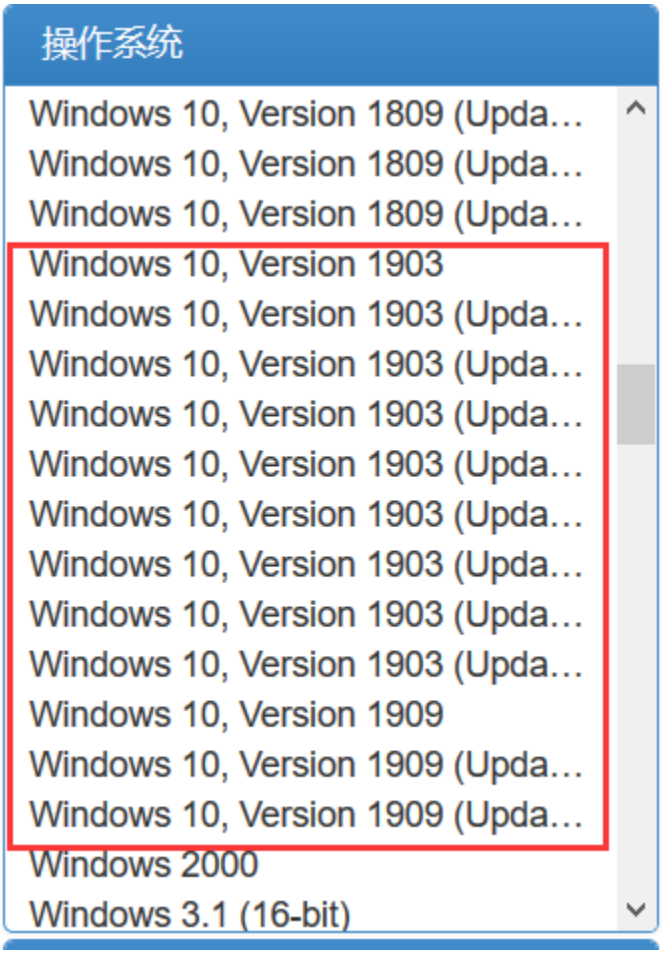
- 适用于32位系统的Windows 10版本1903
  Windows 10 1903版（用于基于x64的系统）
  Windows 10 1903版（用于基于ARM64的系统）
  Windows Server 1903版（服务器核心安装）

- 适用于32位系统的Windows 10版本1909
  Windows 10版本1909（用于基于x64的系统）
  Windows 10 1909版（用于基于ARM64的系统）
  Windows Server版本1909（服务器核心安装）

0x04 环境搭建

下载地址：

https://msdn.itellyou.cn/



0x05 漏洞检测

Python脚本：

https://github.com/ollypwn/SMBGhost/blob/master/scanner.py

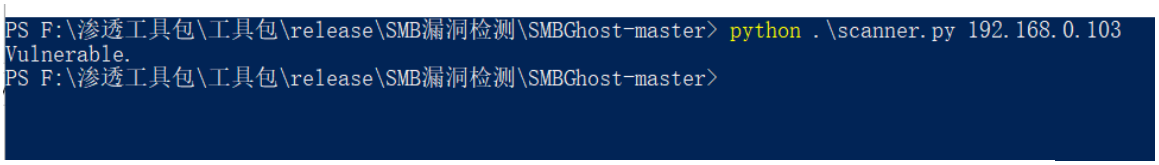
Nmap检测脚本(nse脚本)

https://github.com/cyberstruggle/DeltaGroup/blob/master/CVE-2020-0796/CVE-2020-0796.nse

Powershell检测脚本

https://github.com/T13nn3s/CVE-2020-0976/blob/master/CVE-2020-0796-Smbv3-checker.ps1

解压之后运行scaner.py 文件



0x06 修复方式

1. 安装补丁

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

2. 禁用SMBv3压缩

3. 禁用powershell命令压缩功能

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

参考链接：

https://nosec.org/home/detail/4309.html

https://mp.weixin.qq.com/s/giMOLmGYpgCGbDZb-9xesA
https://mp.weixin.qq.com/s/zTKRkObrUaHq-8eI2HQpDg

阅读原文查看更多复现文章

The end

悄悄点**在看**，技术变精湛!

精选留言

用户设置不下载评论

阅读全文