Ladon Scan SMBGhost CVE-2020-0796 RCE Vulnerable

LPE (/categories/LPE/) Ladon (/categories/Ladon/) Rce (/categories/Rce/)

CVE-2020-0796 (/tags/CVE-2020-0796/) Ladon (/tags/Ladon/) Rce (/tags/Rce/) SMBGhost (/tags/SMB

2020/06/03 142

漏洞介绍

2020年3月10日，微软在其官方SRC发布了CVE-2020-0796的安全公告（ADV200005，MicrosoftGuidance for Disabling SMBv3 Compression），公告表示在Windows SMBv3版本的客户端和服务端存在远程代码执行漏洞。同时指出该漏洞存在于MicroSoft Server Message Block 3.1.1协议处理特定请求包的功能中，攻击者利用该漏洞可在目标SMB Server或者Client中执行任意代码。

影响版本

CVE-2020-0796漏洞影响运行Windows 10版本1903，Windows Server版本1903（服务器核心安装），Windows 10版本1909和Windows Server版本1909（服务器核心安装）的设备。根据Fortinet，其他Microsoft版本应受到影响。

模块说明

漏洞编号：CVE-2020-0796
漏洞别名：SMBGhost
影响版本：Win10或2016 1903 | 1909

结果：IP、机器名、漏洞编号、操作系统版本

无损扫描

通过检测SMB3.1.1是否启用压缩功能判定漏洞，和MS17010一样不会对目标造成任何损害，也不会被杀软拦截。MS17010的影响比这个远大一万倍而且已经公开了3年，前不久还有人反馈目标内网有杀软，但他们依旧能用Ladon扫描出MS17010漏洞，只是EXP不定能用。这个和SQL注入一样，执行命令要比只能SELECT信息要严重要高危，执行命令被拦截正常，如果执行命令都不拦截，AND 1+1它拦截不是脑残吗？有人用NSA原版发那么多包都到了注入DLL那一步，Ladon只发一个包检测MS17010，别人说流量大，这个就像只AND 1+1和1+2检测，说流量大，说得好像Ladon会把系统搞崩或被发现一样，你用个WVS扫描IP发几百上万个包，或者NMAP无脑扫全端口这TM才流量大，WVS和NMAP包里加有固定特征，流量又大你都敢用，都不怕被WAF拦或管理员发现，你和我说Ladon流量大，瞎搞的吧，最简单的抓包都不懂吗？只会造谣瞎扯淡？再不懂往虚拟机安装相关杀软或WAF，再用工具扫描看哪个被报。NMAP和WVS这种公开10几年的扫描都不拦的，Ladon更不可能被拦。

SMBGhost漏洞检测

扫描指定主机SMBGhost漏洞

Ladon 192.168.1.8 SMBGhost

扫描C段主机SMBGhost漏洞

Ladon 192.168.1.8/24 SMBGhost
Ladon 192.168.1.8/C SMBGhost

批量扫描IP列表主机SMBGhost漏洞

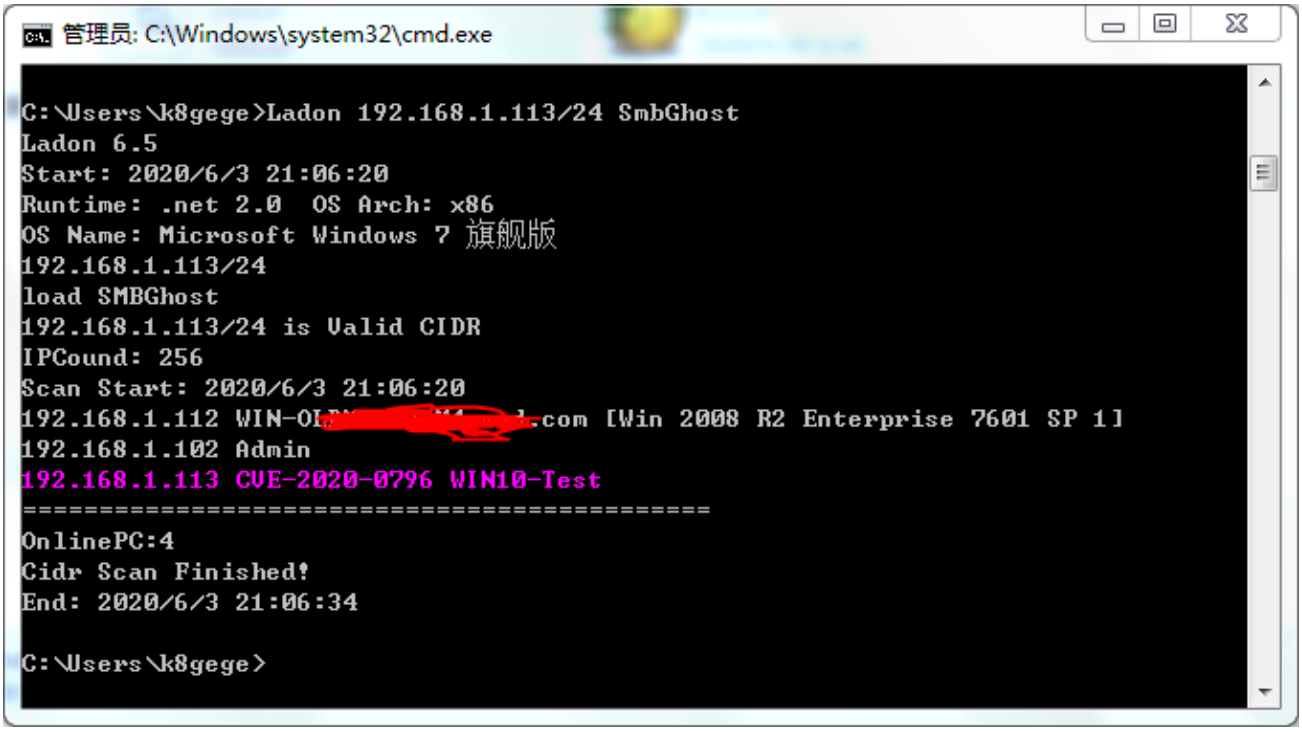
ip.txt里放需要扫描的IP，使用以下命令即可
Ladon SMBGhost

批量检测IP段（/24）SMBGhost漏洞

ip24.txt里放需要扫描的IP段，使用以下命令即可
Ladon SMBGhost

批量检测IP段（/16）SMBGhost漏洞

ip16.txt里放需要扫描的IP段，使用以下命令即可
Ladon SMBGhost



POC/EXP/LPE

https://github.com/danigargu/CVE-2020-0796 (https://github.com/danigargu/CVE-2020-0796)
https://github.com/chompie1337/SMBGhost_RCE_PoC (https://github.com/chompie1337/SMBGhost_RCE_PoC)

工具下载

最新版本：https://k8gege.org/Download/Ladon.rar (https://k8gege.org/Download/Ladon.rar)
历史版本: https://github.com/k8gege/Ladon/releases (https://github.com/k8gege/Ladon/releases)

~进群讨论

下一篇 › (/p/648af4b3.html)