安天周观察
2020 3 23 (223) 4 antiylab

DLL	

COD

0451-86219018 / 010-82893723

2020 3 11 3 Server Message Block 3.1.1 SMBv3 CVE-2020-0796 CVE-2020-0796

SMBv3

SMBv3

Github

Windows 10 Version 1903 for 32-bit Systems

Windows 10 Version 1903 for x64-based Systems

Windows 10 Version 1903 for ARM64-based Systems

Windows Server, Version 1903 (Server Core installation)

Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1909 for x64-based Systems

Windows 10 Version 1909 for ARM64-based Systems

Windows Server, Version 1909 (Server Core installation)

SMB 3.1.1

Windows 10 1903 2019 5 mrxsmb20.sys srv2.sys srvnet.sys srv2.sys

SMB 3.1.1

srv2.sys SrvNetAllocateBuffer srvnet.sys

OriginalSize Offset unsigned int OriginalSize offset unsigned int

https://www.catalog.update.microsoft.com/Search.aspx?q=KB4551762

SMBv3

CVE-2020-0796

https://bbs.antiy.cn/forum.php?mod=viewthread&tid=83848

PowerShell

SMBv3

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

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

SMB

TrickBot RDP

New TrickBot Module Bruteforces RDP Connections, Targets Select Telecommunication Services in US and Hong Kong

Liviu ARSENE&Radu Tudorica&Alexandru MAXIMCIUC&Cristina VATAMANU

Bitdefender 1 30 TrickBot rdpScanDll RDP TrickBot C2 C2 rdpScanDll Check RDP TryBute /RDP/ names /RDP/dict

TrickBot TrickBot C2 C2 IP 16

https://labs.bitdefender.com/2020/03/new-trickbot-module-bruteforces-rdp-connections-targets-select-telecommunication-services-in-us-and-hong-kong/