Dragon Advance Tech

Suite 701-702, 7/F, Shun Feng International Centre, No. 182 Queen's Road East, Wanchai, Hong Kong
Phone +852 2868 6182 Email: admin@dragonadvancetech.com

CVE-2019-0708: RDP Remote Code Execution

TLP:GREEN

[update on: May 23, 2019]

Hong Kong SMEs' Internet facing RDP services are subject to cve-2019-0708 attacks
The vulnerability is also named as #BlueKeep

The vulnerability is believed first found by National Cyber Security Center (NCSC) in UK. (https://www.ncsc.gov.uk/report/weekly-threat-report-17th-may-2019). As of May 17, NCSC observed no exploit of this vulnerability, however, they pose it as a serious threat. Microsoft have taken the unusual step of providing a security updates for all customers to all customers to protect Windows platforms, including some out-of-support version of Windows, including Windows XP and Windows Server 2003. As of May 23, 2019 McAfee, Team was believed to have the exploit called bluekeep[.]exe.

The Time is fulfilled, repent and believe…!

Systems Affected

Microsoft Windows Server 2003, Microsoft Windows XP, Windows 7, Windows Server 2008 and Windows Server 2008 R2. ***[Windows 8 or above is not affected.]***

The Story

On May 14, 2019, Microsoft published an advisory (https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/) announced a newly discovered remote code execution vulnerability, which is identified as CVE-2019-0708. This vulnerability has been named #BlueKeep, by Kevin Beaumont as it's about Red Keep in Game of Thrones.

The vulnerability is believed first found by National Cyber Security Center (NCSC) in UK. (https://www.ncsc.gov.uk/report/weekly-threat-report-17th-may-2019). As of May 17, NCSC observed no exploit of this vulnerability, however, they pose it as a serious threat. ***Microsoft have taken the unusual step*** of providing a security updates for all customers to all customers to protect Windows platforms, including some out-of-support version of Windows, including ***Windows XP*** and ***Windows Server 2003***. Patches can be found at Microsoft Support site. (https://support.microsoft.com/en-hk/help/4500705/customer-guidance-for-cve-2019-0708)

Immediate after the discovery of this vulnerability, script kiddies are publishing their POC in github and someone even registered a domain cve-2019-0807[.]com to deploy a POC exploit which has been ***identified as malicious*** by CrowdStrike's Falcon Sandbox. (https://www.hybrid-analysis.com/sample/02040daef2d25229b36319d6254d66a1e89f8ab69be3c3faddcd903ae4ebcdfe). PLEASE don't try to download any POC scripts from the Internet for fixing your system, unless it is coming directly from Microsoft.

Based on Microsoft's MSRC Team advisory, some in-support systems, including Windows 7, Windows Server 2008 R2 and Windows server 2008 are vulnerable and the patch/hotfix can be found in the Microsoft Security Update Guide. (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708)

HKCERT has also issued a security bulletin on May 15, 2019 updated this vulnerability's criticality level from Medium to High on May 18, 2019. DAT support such claim not only because of POC may be developed and it's worm-like outbreak. It is comparable to the SMB exploits called ***ETERNALBLUE*** (which was made well-known because of WannaCry) found in April-May 2017. The exploit was believed to be embedded inside a kernel system driver called termdd.sys. If any malicious code was successfully executed because of this vulnerability, there is no anti-virus program or defensive tools can effectively detect the malicious code.

The NCSC recommends that organizations and individuals ***apply Microsoft's May security patches ASAP***. In particular organizations should focus on the following:

- External facing RDP severs
- Critical servers such as domain controllers and management servers
- Non-critical servers but those with RDP enabled
- The rest of the desk top estate

In our view, basically all affected Windows systems need to be patched especially for those SME in Hong Kong because in the past we have identified many incidents that SMEs are usually out-sourced their IT supports to the IT Specialists whom may make their clients' system facing the Internet for carrying out their support duties.

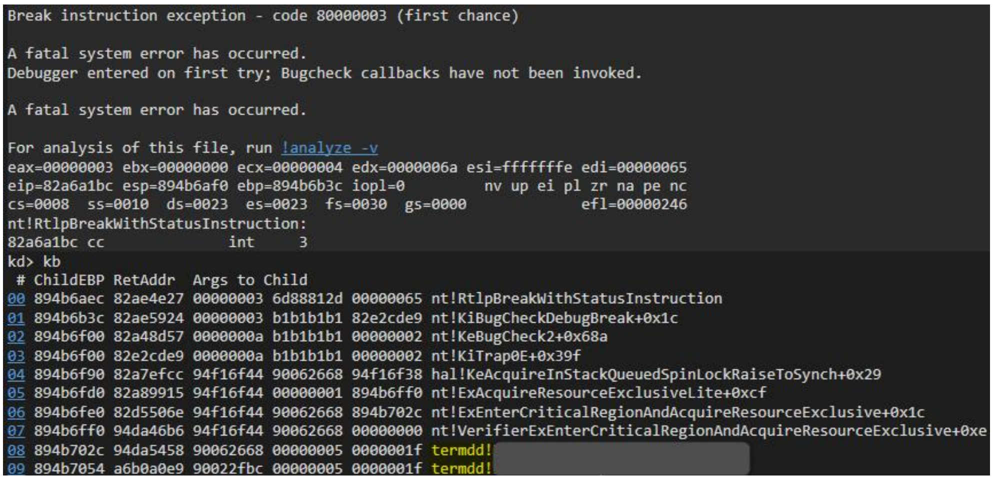
High risk organizations also including Hospitals, Clinics or even organisations that using OT systems and smart devices because some of these devices are running in out-support Windows systems. Those organisations should take immediate steps and follow the best practice as mentioned in this blog.

(https://www.cybermdx.com/blog/how-to-protect-your-hospital-against-bluekeep?hs_amp=true&__twitter_impression=true)

For those organizations who do not have RDP servers exposed to the Internet, they are advised not to overlook the consequent of this vulnerability because don't forget the *lesson learnt from WannaCry,* at first this ransomware affect only SMBv1. DAT recommend even you believe your network was protected by firewall, you need to consider to update the patch or carry out countermeasures to protect your Windows systems.

At the time of this white paper, we have not found effective security solutions that can detect if any systems have been compromised but such vulnerability.

In the past few days, Qualys published a patch detection QID, 360 tried to provide a tool to detect the exploit (http://www.360.cn/n/10666.html) and NTT published a Suricata rules to detect the network activities of rdp. (https://github.com/nccgroup/Cyber-Defence/blob/master/Signatures/suricata/2019_05_rdp_cve_2019_0708.txt) However, none of them can really effectively detect the exact exploit, except, I believe McAfee Team had created a POC exploit and they published a very detailed technical write up. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/



```
Break instruction exception - code 80000003 (first chance)

A fatal system error has occurred.
Debugger entered on first try; Bugcheck callbacks have not been invoked.

A fatal system error has occurred.

For analysis of this file, run !analyze -v
eax=00000003 ebx=00000000 ecx=00000004 edx=0000006a esi=fffffffe edi=00000065
eip=82a6a1bc esp=894b6af0 ebp=894b6b3c iopl=0         nv up ei pl zr na pe nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000             efl=00000246
nt!RtlpBreakWithStatusInstruction:
82a6a1bc cc              int     3
kd> kb
 # ChildEBP RetAddr  Args to Child
00 894b6aec 82ae4e27 00000003 6d88812d 00000065 nt!RtlpBreakWithStatusInstruction
01 894b6b3c 82ae5924 00000003 b1b1b1b1 82e2cde9 nt!KiBugCheckDebugBreak+0x1c
02 894b6f00 82a48d57 0000000a b1b1b1b1 00000002 nt!KeBugCheck2+0x68a
03 894b6f00 82e2cde9 0000000a b1b1b1b1 00000002 nt!KiTrap0E+0x39f
04 894b6f90 82a7efcc 94f16f44 90062668 94f16f38 hal!KeAcquireInStackQueuedSpinLockRaiseToSynch+0x29
05 894b6fd0 82a89915 94f16f44 00000001 894b6ff0 nt!ExAcquireResourceExclusiveLite+0xcf
06 894b6fe0 82d5506e 94f16f44 90062668 894b702c nt!ExEnterCriticalRegionAndAcquireResourceExclusive+0x1c
07 894b6ff0 94da46b6 94f16f44 90062668 00000000 nt!VerifierExEnterCriticalRegionAndAcquireResourceExclusive+0xe
08 894b702c 94da5458 90062668 00000005 0000001f termdd![redacted]
09 894b7054 a6b0a0e9 90022fbc 00000005 0000001f termdd!
```

"IT CAN HAPPEN TO ANYONE AND MAY HAPPEN AGAIN"

The Time is fulfilled, repent and believe…!