H-ISAC TIC Vulnerability Bulletin

Date: 7/24/2019 (originally issued 5/14/2019)

TLP – WHITE

Event: Update: CVE-2019-0708 Remote Desktop Services Remote Code Execution Vulnerability

Update Notes:

1. More manufacturers added to the attached appendix along with a link to their public advisory
2. Added mention of availability of Immunity CANVAS exploit module.

Summary: On May 14th, 2019 Microsoft released a security advisory[1] and patches for the CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability" now commonly known as "BlueKeep." The vulnerability affects RDP services for Windows 2000, Windows XP, Server 2003, Vista, Server 2008, 7, and Server 2008 R2. It's likely that it also affects Windows CE and older operating systems. It does NOT affect Windows 8, Server 2012, and newer operating systems. It can be exploited remotely, in default configuration, and without any authentication or user interaction. We assess that this vulnerability is high risk to all H-ISAC member organizations and is very likely to have significant impact. We also expect to see significant secondary impact as many members of our ecosystem of hospitals, clinics, doctors, and third-party vendors have vulnerable systems exposed to the internet.

Microsoft released patches[1] for affected operating systems, including some currently out of support[2] such as Windows XP, Server 2003, and Vista. In scenarios where a patch cannot be applied, the vulnerability can be partially mitigated by enabling the NLA (Network Level Authentication) required option in RDP server configuration. Microsoft previously stated[3] they are "confident that an exploit exists for this vulnerability" and has posted blogs[3,4] warning customers to patch along with the Canadian Centre for Cyber Security (CCCS)[5], UK National Cyber Security Centre (NCSC)[6,7], US National Security Agency (NSA)[8] and US Cybersecurity and Infrastructure Security Agency (CISA)[9]. Many medical device manufacturers have also released public advisories and are listed in the Appendix.

The only requirement for exploitability is the ability to communicate with the RDP server. Multiple individuals and groups at Zerodium, McAfee, Qihoo 360, RiskSense, Sophos, and others have privately developed working Remote Code Execution (RCE) exploits, but have not made them publicly available. Immunity has an exploit module in their CANVAS product. No active exploitation has been observed in the wild at this time, but there are publicly available exploits that can cause Denial of Service (DoS).

Most vulnerability scanning vendors[10,11] should be able to detect the presence of the associated KBs and remotely detect the vulnerability and if Network Level Authentication is required or not. There are also multiple dedicated tools[12,13,14] to detect the vulnerability including a Metasploit module[15]. Many security vendors have partial "signatures" for detecting/preventing exploitation but they only work when not using TLS which some Proof of Concept (PoC) exploits are starting to use. Members should consult with their respective endpoint security & vulnerability scanning vendors for further information. There are multiple Internet search engines and reporting services[16,17,18,19] that can help to identity external RDP servers, but be aware that some ISPs block them so they may not be comprehensive.

Assessment: There's a remotely exploitable, wormable, pre-authentication vulnerability in a very popular server (initial reporting showed almost 1 million vulnerable RDP servers accessible on the Internet). The healthcare vertical makes heavy use of internet-facing RDP servers to enable various business and support functions. It is likely that significant vertical-wide disruptions will occur when the exploit is eventually made public.

Recommended Course of Action (COA):

- Consider requiring Network Level Authentication as an immediate short-term partial mitigation or disabling RDP on systems that don’t require it.
- Execute emergency patching procedure. Ensure external and internal systems are fully patched.
- Consider any network links with third-parties and assess potential impact if the third party should be compromised.
- Identify external assets with RDP enabled and remediate immediately.
- Contact supply chain partners to ensure affected devices are patched.

References:

1. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
2. https://support.microsoft.com/help/4500705
3. https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/
4. https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
5. https://cyber.gc.ca/en/alerts/critical-microsoft-remote-desktop-vulnerability
6. https://www.ncsc.gov.uk/report/weekly-threat-report-17th-may-2019
7. https://www.ncsc.gov.uk/report/weekly-threat-report-31st-may-2019
8. https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/
9. https://www.us-cert.gov/ncas/alerts/AA19-168A
10. https://blog.qualys.com/laws-of-vulnerabilities/2019/05/15/windows-rdp-remote-code-execution-vulnerability-bluekeep-how-to-detect-and-patch
11. https://www.tenable.com/blog/critical-remote-code-execution-vulnerability-cve-2019-0708-addressed-in-patch-tuesday-updates
12. https://github.com/zerosum0x0/CVE-2019-0708
13. https://github.com/robertdavidgraham/rdpscan
14. https://github.com/nccgroup/BKScan/
15. https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep.rb
16. https://blog.binaryedge.io/2019/05/15/rdp-exposed-on-the-internet/

17. https://censys.io/ipv4?q=tags%3Ardp
18. https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
19. https://www.shodan.io/search?query="Remote+Desktop+Protocol"

Questions/Feedback: Please contact contact@h-isac.org

Appendix:

Note: Some manufacturers may have private advisories. Contact manufacturer for guidance. Additional details may also be available from H-ISAC and MDSISC.

Manufacturer	Public Advisory
Abbott	https://www.abbott.com/policies/cybersecurity/microsoft-product-security-bulletin.html
Accuray	https://www.accuray.com/wp-content/uploads/microsoftrdpvulnerabilitycommunication.pdf
Agfa Healthcare	Unknown
AvaSure	Unknown
Baxter	https://www.baxter.com/sites/g/files/ebysai746/files/2019-05/Remote%20Desktop%20Services%20Product%20Security%20Bulletin.pdf
Bayer	Unknown
BD	https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletins/remote-desktop-services-remote-code-execution-vulnerability
Beckman Coulter (Danaher)	https://www.beckmancoulter.com/en/about-beckman-coulter/product-security/product-security-updates
bioMérieux	https://www.biomerieux-usa.com/product-security
BK Medical	Unknown
Boston Scientific	https://www.bostonscientific.com/content/dam/bostonscientific/corporate/product-security/BSC-Statement-on-Microsoft-BlueKeep-Vulnerability.pdf
Brainlab	Unknown
Canon	https://us.medical.canon/download/Canon_Security_Advisory_RDP_CVE_2019_0708
Capintec	Unknown
Capsule Technologies	Unknown
Carestream	https://www.carestream.com/en/us/-/media/publicsite/resources/service-and-support-publications/product-security-advisory-cve-2019-0708-bluekeep.pdf
Carl Zeiss Meditec	Unknown
Cepheid (Danaher)	http://www.cepheid.com/us/product-security
Change Healthcare (McKesson)	Unknown
Draeger	https://static.draeger.com/security/download/2019-05-16-Windows-RDP-RCE-for-CVE-2019-0708-Security-Advisory.pdf
Foresight Imaging	Unknown
Fujifilm Medical	https://extranet.fujimed.com/ (credentials required)
GE Healthcare	https://www.gehealthcare.com/en/support/security-information
Hillrom	Unknown
Hitachi Healthcare	Unknown
Hologic	https://www.hologic.com/package-inserts
iCAD	Unknown
Johnson & Johnson	https://www.productsecurity.jnj.com/advisories.html

Manufacturer	Public Advisory
KARL STORZ	PDF available via Medical Device Security Information Sharing Council (MDSISC)
KaVo (Danaher)	Unknown
Konica Minolta	Unknown
Medtronic	https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-security-bulletin_RDP_052819.pdf
Merge Healthcare (IBM)	https://www.merge.com/Support/Resources/Security-Patches.aspx
Molecular Devices (Danaher)	https://mdc.custhelp.com/app/answers/detail/a_id/20814
Natus	Unknown
Nihon Kohden	https://us.nihonkohden.com/it-solutions/cybersecurity/
Nova Biomedical	Unknown
Olympus	https://medical.olympusamerica.com/sites/default/files/us/files/pdf/Microsoft-Remote-Desktop-Services-Communication.pdf
Parks Medical Electronics	Unknown
Philips	https://www.usa.philips.com/healthcare/about/customer-support/product-security
Radiometer (Danaher)	Unknown
Roche	Unknown
Samsung Healthcare	Unknown
ScottCare	Unknown
Siemens	https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications
Smiths Medical	Unknown
SonoSite (Fujifilm)	https://www.sonosite.com/support/cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability
Spacelabs Healthcare (OSI Systems)	Unknown
Stanley Healthcare	Unknown
Stryker	https://www.stryker.com/us/en/about/governance/cyber-security/product-security/microsoft-windows-rdp-vulnerability--cve-2019-0708--bulletin.html
Sysmex	Unknown
Vital Images (Canon)	https://www.vitalimages.com/customer-success-support-program/vital-images-software-security-updates/
Vyaire Medical	https://www.vyaire.com/sites/default/files/2019-06/Security%20bulletin%20for%20vulnerability%20-%20BlueKeep.pdf