H-ISAC TIC Vulnerability Bulletin

Date: 6/7/2019 (originally issued 5/14/2019)

TLP – WHITE

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

Summary: On May 14th, 2019 Microsoft released a security advisory[1] for CVE-2019-0708 "Remote Desktop Services Remote Code Execution Vulnerability" now commonly known as "BlueKeep". The vulnerability affects RDP services for Windows XP, Server 2003, Vista, Server 2008, 7, and Server 2008 R2. It's likely that it also affects Windows 2000, 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 is confident that an exploit exists for this vulnerability"[3] and has posted blogs[3,4] warning customers to patch along with the US National Security Agency (NSA)[5] and UK National Cyber Security Centre (NCSC). Many medical device manufacturers have also released 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, and RiskSense have developed working Remote Code Execution (RCE) exploits including a Metasploit module, but none have made them publicly available at this time. However there are exploits that can cause Denial of Service (DoS) that are public. No active exploitation has been observed in the wild at this time.

Most vulnerability scanning vendors[6,7] 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[8,9] to detect the vulnerability including a Metasploit module[10]. 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[11,12,13,14] 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 (recent reporting shows 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://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/
6. https://blog.qualys.com/laws-of-vulnerabilities/2019/05/15/windows-rdp-remote-code-execution-vulnerability-bluekeep-how-to-detect-and-patch
7. https://www.tenable.com/blog/critical-remote-code-execution-vulnerability-cve-2019-0708-addressed-in-patch-tuesday-updates
8. https://github.com/zerosum0x0/CVE-2019-0708
9. https://github.com/robertdavidgraham/rdpscan
10. https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep.rb
11. https://blog.binaryedge.io/2019/05/15/rdp-exposed-on-the-internet/
12. https://censys.io/ipv4?q=tags%3Ardp
13. https://www.shadowserver.org/what-we-do/network-reporting/get-reports/
14. https://www.shodan.io/search?query=%22Remote+Desktop+Protocol%22

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

Appendix:

Manufacturer	Advisory
Abbott	https://www.abbott.com/policies/cybersecurity/microsoft-product-security-bulletin.html
Accuray	https://www.accuray.com/wp-content/uploads/microsoftrdpvulnerabilitycommunication.pdf
Baxter	https://www.baxter.com/sites/g/files/ebysai746/files/2019-05/Remote%20Desktop%20Services%20Product%20Security%20Bulletin.pdf
BD	https://www.bd.com/en-us/support/product-security-and-privacy/product-security-bulletins/remote-desktop-services-remote-code-execution-vulnerability
Beckman Coulter	https://www.beckmancoulter.com/en/about-beckman-coulter/product-security/product-security-updates
Boston Scientific	https://www.bostonscientific.com/content/dam/bostonscientific/corporate/product-security/BSC-Statement-on-Microsoft-BlueKeep-Vulnerability.pdf
Canon	https://us.medical.canon/download/Canon_Security_Advisory_RDP_CVE_2019_0708
Carestream	https://www.carestream.com/en/us/-/media/publicsite/resources/service-and-support-publications/product-security-advisory-cve-2019-0708-bluekeep.pdf
Draeger	https://static.draeger.com/security/download/2019-05-16-Windows-RDP-RCE-for-CVE-2019-0708-Security-Advisory.pdf
GE Healthcare	https://www.gehealthcare.com/en/support/security-information
KARL STORZ	PDF available via Medical Device Security Information Sharing Council (MDSISC)
Medtronic	https://www.medtronic.com/content/dam/medtronic-com/us-en/corporate/documents/Medtronic-security-bulletin_RDP_052819.pdf
Olympus	https://medical.olympusamerica.com/sites/default/files/us/files/pdf/Microsoft-Remote-Desktop-Services-Communication.pdf
Philips	https://www.usa.philips.com/healthcare/about/customer-support/product-security
Siemens	https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications
Stryker	https://www.stryker.com/us/en/about/governance/cyber-security/product-security/microsoft-windows-rdp-vulnerability--cve-2019-0708--bulletin.html