DARKMATTER

DARKMATTER ADVISORY – CRITICAL VULNERABILITIES IN REMOTE DESKTOP SERVICES

19 AUGUST 2019

SMART AND SAFE DIGITAL

Executive Summary

Two new vulnerabilities affecting Microsoft Windows' Remote Desktop Services that could be leveraged by worms were disclosed via Microsoft's Patch Tuesday on 13 August 2019[1]. The vulnerabilities were included in a list of 93 vulnerabilities patched by Microsoft's latest security[2] updates. Remote Desktop Services is a ubiquitous network service among organisations and even personal desktops.

The known existence of these vulnerabilities could lead to the development of self-propagating malware that would pose a significant threat to organisations with public facing Microsoft Windows machines. Without applying Microsoft's 13 August 2019 security updates, organisations face a rising risk of incidents by threat actors looking to leverage the critical vulnerabilities. Various security researchers, to include those at Tencent, are currently developing proof of concept exploits.

DarkMatter has observed thousands of hosts belonging to UAE organisations where Remote Desktop Services are publicly exposed. Such exposure, means any vulnerable machines face rising threats as threat actors work to develop exploits against the new vulnerabilities.

TIC ANALYSIS

Microsoft disclosed via a 13 August 2019 release of security updates that four vulnerabilities: CVE-2019-1181[3], CVE-2019-1182[4] , CVE-2019-1222[5] , and CVE-2019-1226[6] ; existing in Remote Desktop Services were patched. Although the published descriptions for all four vulnerabilities are identical, namely allowing for remote code execution without an authenticated remote desktop session, Microsoft singled out two, CVE-2019-1181 and CVE-2019-1182, for being "wormable" in a blog post[7]. Microsoft did not publish why these two vulnerabilities were highlighted despite identical descriptions to the other two vulnerabilities fixed in the same patch release.

Both CVE-2019-1181 and CVE-2019-1182 allow an attacker with an established remote desktop session to execute arbitrary code prior to authentication to the targeted machine. Both vulnerabilities received a base score of 9.8 (critical) from the Common Vulnerability Scoring System (CVSS). Security researchers are already working to develop proof of concept exploits against the vulnerabilities. Researchers at Tencent[8], for example, claimed they have developed a successful exploit, but have not provided further details outside of a video demonstration showing an apparent denial of service effect rather than remote code execution. Other researchers have likewise claimed successfully crashing the remote desktop hosts thus far exploiting the two vulnerabilities.

One of the potential threats from the stated vulnerabilities would be the development of a worm that spreads via exploits against either of the vulnerabilities. As worms can propagate on their own over the Internet, an exploit that does not require human interaction against common network services can quickly cause widespread damage to organisations around the world. As Remote Desktop Services are commonly exposed to the Internet and CVE-2019-1181 and CVE-2019-1182 can be exploited without the need of a victim's interaction, an operational exploit could lead to prolific damage.

While an attacker does not need to authenticate to a remote desktop host in order to exploit the vulnerabilities, an attacker may require network authentication should the targeted host require Network Level Authentication prior to establishing a remote desktop session. For this reason, enabling Network Level Authentication for any remote desktop connection mitigates the inbound threats specifically from self-propagating malware. However, vulnerable machines would still face significant threats from targeted attacks where compromised credentials are more likely to be leveraged.

DarkMatter has reviewed the attack surface of the UAE and has identified at least 3373 unique hosts where Remote Desktop Services are publicly exposed. Some of these hosts belong to government organisations that already face persistent threats from around the world. Without applying the security updates, these vulnerable systems could be compromised remotely from the Internet using the stated vulnerabilities.

RECOMMENDED ACTIONS

The DarkMatter Threat Intel Center recommends the following measures:

- Strictly follow a vulnerability management process to ensure organisation assets are routinely patched. Microsoft follows a formalized cadence of releasing patches that address critical security flaws such as CVE-2019-1181 and CVE-2019-1182 at least one Tuesday every month.

- Enforce Network Level Authentications for Remote Desktop Services on all organisation machines. Network Level Authentication would help mitigate risks presented by such vulnerabilities even prior to public disclosure. Such measure would require an individual to first successfully authenticate to an organisation's network, prior to being able to establish a remote desktop session with a targeted machine.

- Block inbound access to TCP and UDP ports 3389 from any unauthorized networks. Services that allow remote administration of machines, such as Remote Desktop Services, are highly sought after by threat actors. Needless exposure of these services only provide threat actors with a greater attacker surface against which to stage their attacks. By blocking inbound access to port 3389 at the firewall, an organisation limits a threat actor's ability to target vulnerable machines.

REFERENCES

1 Microsoft (13 August 2019) August 2019 Security Updates. Retrieved from https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/312890cc-3673-e911-a991-000d3a33a34d

2 SANS ISC InfoSec Forums (13 August 2019) August 2019 Microsoft Patch Tuesday. Retrieved from https://isc.sans.edu/forums/diary/August+2019+Microsoft+Patch+Tuesday/25236/

3 Microsoft (13 August 2019) CVE-2019-1181 | Remote Desktop Services Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181

4 Microsoft (13 August 2019) CVE-2019-1182 | Remote Desktop Services Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182

5 Microsoft (13 August 2019) CVE-2019-1222 | Remote Desktop Services Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222

6 Microsoft (13 August 2019) CVE-2019-1226 | Remote Desktop Services Remote Code Execution Vulnerability. Retrieved from https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

7 Microsoft (13 August 2019) Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182). Retrieved from https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/

8 Tencent (15 August 2019) Vulnerability Alert Update: August Windows RDS Vulnerability (CVE-2019-1181, CVE-2019-1182). Retrieved from https://s.tencent.com/research/bsafe/778.html

Contact Us

Should you need additional details, you can reach out to us at contactus@darkmatter.ae.