CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-013

Remote Desktop Services – Remote Code Execution Vulnerability

July 24, 2019 — v1.1

TLP:WHITE

History:

- *16/05/2019 — v1.0 – Initial publication*
- *24/07/2019 — v1.1 – Additional information about exploits and patches for older versions of Windows available*

Summary

Microsoft released fixes for a critical Remote Code Execution vulnerability (CVE-2019-0708) in Remote Desktop Services that affects some older versions of Windows. The vulnerability has been since named **BlueKeep**. The Remote Desktop Protocol (RDP) itself is not vulnerable. This vulnerability is pre-authentication and requires no user interaction. In other words, the vulnerability is *wormable*, meaning that any malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017 [1]. Exploits seem to already exist [4, 5, 6].

Technical Details

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploits this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP [2]. Exploit seems relatively easy [4, 5, 6] so the attacks are probably imminent. Also, the exploits are being now included in popular exploit development frameworks, such as CANVAS [6, 7].

Products Affected

- Vulnerable supported systems include Windows 7, Windows Server 2008 R2, and Windows Server 2008.
- Vulnerable out-of-support systems include Windows 2003 and Windows XP.
- Windows 8 and Windows 10 are not affected by this vulnerability.

Recommendations

Downloads for supported versions of Windows can be found in the Microsoft Security Update Guide [2]. Customers who use a supported version of Windows and have automatic updates enabled are automatically protected. Customers who use an out-of-support version should address this vulnerability by upgrading to the latest version of Windows. Even so, Microsoft is making fixes available for these out-of-support versions of Windows in KB4500705 [3].

Microsoft has exceptionally also issued patches for older, out of support versions of the Windows operating system including XP, Vista, and Server 2003. They can be found in [8].

In all cases, Microsoft strongly recommends to install the updates for this vulnerability as soon as possible even if you plan to leave Remote Desktop Services disabled.

Workarounds

The following workarounds may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if you plan to leave these workarounds in place:

- Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2

You can enable Network Level Authentication to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability.

- Block TCP port 3389 at the enterprise perimeter firewall

TCP port 3389 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter.

References

[1] https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[3] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

[4] https://twitter.com/cBekrar/status/1128712967845961728

[5] https://arstechnica.com/information-technology/2019/07/explainer-for-exploiting-wormable-bluekeep-flaw-posted-on-github/

[6] https://twitter.com/Immunityinc/status/1153752470130221057?s=19

[7] https://www.immunityinc.com/products/canvas/

[8] https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708