American
Technology Services
a WWTS Company

2019-01 ATS Security Advisory

Windows Remote Desktop Vulnerability

Summary

On Tuesday May 14th, 2019, Microsoft's Security Response Center released a statement along with a patch for a critical Remote Code Execution vulnerability in Remote Desktop Services.[i] The vulnerability affects Windows Server versions 2008 R2, 2008, and 2003. Windows 7 and XP are also affected.

If exploited, an attacker can execute code on a vulnerable system before authentication occurs, allowing them to fully compromise the system. Public-facing Remote Desktop servers pose the largest initial risk to organizations, though all other vulnerable systems still pose a significant risk. Certain mitigations can be put in place to force an attacker to have valid credentials to the vulnerable system to exploit it. The only way to prevent exploitation is by installing the patch provided by Microsoft. [ii]

Details

Microsoft has not provided specific details on the vulnerability and proof-of-concept (PoC) code is not yet publicly available. This will most likely not be the case for long. Once an exploit is widely available, this vulnerability has the potential to be 'wormable', as it can be exploited without credentials of any kind. Prevention of wide-spread exploitation relies on the immediate patching of vulnerable systems.

It should be noted that Microsoft support for the affected versions of Windows (Server 2008, 2008 R2 and 7) ends on January 14, 2020. A plan should be in place to upgrade systems running these versions before that date.

What Can You Do?

The ATS Network Operation Center (NOC) began deploying the patch for this vulnerability to all Managed Services clients outside of the regular patch cycle, due to the critical nature of the vulnerability. All affected operating systems are in the process of installing the patch, no further action is required.

Clients that are not under a Managed Services contract should install the patch immediately. Alternatively, there are a few mitigation and workaround options that Microsoft suggests:

1. **Disable Remote Desktop Services if not required.**
2. Where RDP is required, place it behind a corporate VPN.
3. Enable Network Level Authentication for all Remote Desktop systems.
    a. This is a highly suggested step regardless of this vulnerability.
4. Block the Microsoft RDP port (TCP 3389) at the perimeter firewall.

These mitigations reduce the risk posed by this vulnerability by forcing an attacker to have credentials to the vulnerable system. The only way to prevent exploitation is by installing the patch.

For more information or assistance in assuring your systems are not vulnerable, please contact your ATS Client Manager or the helpdesk at 703-876-2653 or helpdesk@networkATS.com.

References:

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

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