Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)

Today Microsoft released fixes for a critical Remote Code Execution vulnerability, CVE-2019-0708, in Remote Desktop Services – formerly known as Terminal Services – that affects some older versions of Windows. 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 future 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. While we have observed no exploitation of this vulnerability, it is highly likely that malicious actors will write an exploit for this vulnerability and incorporate it into their malware.

Now that I have your attention, it is important that affected systems are patched as quickly as possible to prevent such a scenario from happening. In response, we are taking the unusual step of providing a security update for all customers to protect Windows platforms, including some out-of-support versions of Windows.

Vulnerable in-support systems include Windows 7, Windows Server 2008 R2, and Windows Server 2008. Downloads for in-support versions of Windows can be found in the Microsoft Security Update Guide. Customers who use an in-support version of Windows and have automatic updates enabled are automatically protected.

Out-of-support systems include Windows 2003 and Windows XP. If you are on an out-of-support version, the best way to address this vulnerability is to upgrade to the latest version of Windows. Even so, we are making fixes available for these out-of-support versions of Windows in KB4500705.

Customers running Windows 8 and Windows 10 are not affected by this vulnerability, and it is no coincidence that later versions of Windows are unaffected. Microsoft invests heavily in strengthening the security of its products, often through major architectural improvements that are not possible to backport to earlier versions of Windows.

There is partial mitigation on affected systems that have Network Level Authentication (NLA) enabled. The affected systems are mitigated against ‘wormable’ malware or advanced malware threats that could exploit the vulnerability, as NLA requires authentication before the vulnerability can be triggered.

However, affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

It is for these reasons that we strongly advise that all affected systems – irrespective of whether NLA is enabled or not – should be updated as soon as possible.

Resources
Links to downloads for Windows 7, Windows 2008 R2, and Windows 2008
Links to downloads for Windows 2003 and Windows XP

Simon Pope, Director of Incident Response, Microsoft Security Response Center (MSRC)

Skip to main content