NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

PATCH REMOTE DESKTOP SERVICES ON LEGACY VERSIONS OF WINDOWS®

DISCUSSION

The National Security Agency is urging Microsoft Windows administrators and users to ensure they are using a patched and updated system in the face of growing threats. Recent warnings by Microsoft[1] stressed the importance of installing patches to address a vulnerability in older versions of Windows. Microsoft has warned that this flaw is potentially "wormable," meaning it could spread without user interaction across the internet. We have seen devastating computer worms inflict damage on unpatched systems with wide-ranging impact, and are seeking to motivate increased protections against this flaw.

CVE-2019-0708, dubbed "BlueKeep," is a vulnerability in Remote Desktop Services (RDS) on legacy versions of the Windows®[2] operating system. The following versions of Windows® are affected:

- Windows® XP
- Windows Server® 2003
- Windows® Vista
- Windows Server® 2008
- Windows® 7
- Windows Server® 2008 R2

Although Microsoft has issued a patch, potentially millions of machines are still vulnerable. This is the type of vulnerability that malicious cyber actors frequently exploit through the use of software code that specifically targets the vulnerability. For example, the vulnerability could be exploited to conduct denial of service attacks. It is likely only a matter of time before remote exploitation tools are widely available for this vulnerability. NSA is concerned that malicious cyber actors will use the vulnerability in ransomware and exploit kits containing other known exploits, increasing capabilities against other unpatched systems.

MITIGATION ACTIONS

NSA urges everyone to invest the time and resources to know your network and run supported operating systems with the latest patches. This is critical not just for NSA's protection of National Security Systems but for all networks.

To address CVE-2019-0708 immediately apply the following patches for each respective affected version of the Windows® operating system:

- Windows® XP / Windows Server® 2003 – Security Patch KB4500331
- Windows® Vista / Windows Server® 2008 – Security Patch KB4499180 OR Monthly Rollup KB4499149
- Windows® 7 / Windows Server® 2008 R2 – Security Patch KB4499175 OR Monthly Rollup KB4499164

[1] https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/

[2] Windows and Windows Server are registered trademarks of the Microsoft Corporation

In order to increase resilience against this threat while large networks patch and upgrade, there are additional measures that can be taken as described in the Microsoft® CVE-2019-0708 security advisory[3]:

- Block TCP Port 3389 at your firewalls, especially any perimeter firewalls exposed to the internet. This port is used by the Remote Desktop Protocol (RDP) and will block attempts to establish a connection.
- Enable Network Level Authentication. With NLA enabled, attackers would first have to authenticate to RDS in order to successfully exploit the vulnerability. NLA is available on the Windows® 7, Windows Server® 2008 and Windows Server® 2008 R2 operating systems.
- Disable remote Desktop Services if they are not required. Disabling unused and unneeded services helps reduce exposure to security vulnerabilities overall and is a best practice even without the BlueKeep threat.

Note that Windows® 10 systems are already protected from this vulnerability, as it only affects the older versions of Windows® listed above.

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or Otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT

Cybersecurity Requirements Center

410-854-4200

Cybersecurity_Requests@nsa.gov

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