An official website of the United States government Here’s how you know

America’s Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

CYBERSECURITY ADVISORY

Microsoft Operating Systems BlueKeep Vulnerability

Last Revised: June 17, 2019 **Alert Code:** AA19-168A

Give Feedback

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this Activity Alert to provide information on a vulnerability, known as “BlueKeep,” that exists in the following Microsoft Windows Operating Systems (OSs), including both 32- and 64-bit versions, as well as all Service Pack versions:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

An attacker can exploit this vulnerability to take control of an affected system.

Technical Details

BlueKeep (CVE-2019-0708) exists within the Remote Desktop Protocol (RDP) used by the Microsoft Windows OSs listed above. An attacker can exploit this vulnerability to perform remote code execution on an unprotected system.

According to Microsoft, an attacker can send specially crafted packets to one of these operating systems that has RDP enabled.[1 <https://msrc.microsoft.com/update-guide/en-us/advisory/cve-2019-0708>] After successfully sending the packets, the attacker would have the ability to perform a number of actions: adding accounts with full user rights; viewing, changing, or deleting data; or installing programs. This exploit, which requires no user interaction, must occur before authentication to be successful.

BlueKeep is considered “wormable” because malware exploiting this vulnerability on a system could propagate to other vulnerable systems; thus, a BlueKeep exploit would be capable of rapidly spreading in a fashion similar to the WannaCry malware attacks of 2017. [2]

Give Feedback

CISA has coordinated with external stakeholders and determined that Windows 2000 is vulnerable to BlueKeep.

Mitigations

CISA encourages users and administrators review the Microsoft Security Advisory [1 <https://msrc.microsoft.com/update-guide/en-us/advisory/cve-2019-0708>] and the Microsoft Customer Guidance for CVE-2019-0708 [3 <https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-

2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e>] and apply the appropriate mitigation measures as soon as possible:

- **Install available patches.** Microsoft has released security updates to patch this vulnerability. Microsoft has also released patches for a number of OSs that are no longer officially supported, including Windows Vista, Windows XP, and Windows Server 2003. As always, CISA encourages users and administrators to test patches before installation.

For OSs that do not have patches or systems that cannot be patched, other mitigation steps can be used to help protect against BlueKeep:

- **Upgrade end-of-life (EOL) OSs.** Consider upgrading any EOL OSs no longer supported by Microsoft to a newer, supported OS, such as Windows 10.
- **Disable unnecessary services.** Disable services not being used by the OS. This best practice limits exposure to vulnerabilities.
- **Enable Network Level Authentication.** Enable Network Level Authentication in Windows 7, Windows Server 2008, and Windows Server 2008 R2. Doing so forces a session request to be authenticated and effectively mitigates against BlueKeep, as exploit of the vulnerability requires an unauthenticated session.
- **Block Transmission Control Protocol (TCP) port 3389 at the enterprise perimeter firewall.** Because port 3389 is used to initiate an RDP session, blocking it prevents an attacker from exploiting BlueKeep from outside the user's network. However, this will block legitimate RDP sessions and may not prevent unauthenticated sessions from being initiated inside a network.

References

[1] Microsoft Security Advisory for CVE-2019-0708 <https://msrc.microsoft.com/update-guide/en-us/advisory/cve-2019-0708>

[2] White House Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea

[3] Microsoft Customer Guidance for CVE-2019-0708 <https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e>

Revisions

June 17, 2019: Initial version

June 17, 2019: Revised technical details section.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Give Feedback

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov