Microsoft Operating Systems BlueKeep Vulnerability (CSB19-04)

SUMMARY

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.

IMPACT

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. 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.

MITIGATIONS

Install available patches. Microfost 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. Users and administrators are encourage to test patches before installation.

- **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.

REFERENCE

- https://www.us-cert.gov/ncas/alerts/AA19-168A