Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Microsoft Windows Security Vulnerability – 'BlueKeep' (CVE-2019-0708)

Vulnerability

The Australian Signals Directorate's Australian Cyber Security Centre advises Windows users to ensure their systems are patched and up to date after Microsoft's recent disclosure of new remote desktop vulnerability.

CVE-2019-0708, also known as 'BlueKeep' leaves users open to attack from malicious actors who can exploit a vulnerability via Remote Desktop Services (RDS) on legacy versions of the Windows operating system. Malicious actors can utilise this vulnerability on unprotected systems to conduct denial of services attacks, access systems or view, change and delete information.

The vulnerability is present in Windows 7, Windows XP, Server 2003 and 2008. Microsoft issued a patch for these systems, but millions of machines are potentially still vulnerable. Complacency is a big risk factor, as malicious actors do not always act immediately.

Over the weekend of 12 May 2017, the cyberattack known as WannaCry, using the EternalBlue vulnerability, compromised more than 200,000 victims in 150 countries. The vulnerability used older versions of Microsoft Windows to lock users' files and demand ransom to release them.

Of concern, the victims could have avoided the compromise completely as a patch for the EternalBlue vulnerability had been freely available for more than two months.

Further information about CVE-2019-0708 (BlueKeep) is available on Microsoft's website.

To report a cybercrime, visit cyber.gov.au.

Background

Microsoft has advised that a remote code execution vulnerability exists within its Windows Remote Desktop Services (RDS) when an unauthenticated attacker connects to the target system using Remote Desktop Protocols (RDP) and sends specially crafted requests.

The vulnerability requires no user interaction and occurs pre-authentication. Attackers can use this exploitation to execute arbitrary code in target systems and then install programs or create new accounts with full user rights.

An attacker only needs to send a specially crafted request to the target systems RDS, through an RDP, to exploit the vulnerability.

The CVE-2019-0708 update addresses the vulnerability by correcting how Remote Desktop Services handle connection requests.

Impact

A Remote Desktop Protocol (RDP) service left unpatched is likely exposed and potentially exploitable. The BlueKeep vulnerability equally applies to both external and internal facing RDP and can enable malicious actors to move laterally in a network.

Motivated actors are already scanning the Australian environment looking for unpatched systems to exploit.

The BlueKeep vulnerability is readily available to weaponise and exploit as it has no pre-conditions, other than being able to access RDP on an unpatched operating system.

A malicious actor using email or the web as a vector to deliver executable content to a system that calls on internal RDP resources would likely be highly successful and could be just as effective as WannaCry.

Mitigation

The Australian Cyber Security Centre advises Windows users to:

- Patch as soon as possible
  - Microsoft patching options are available here for the following systems:
    - Windows 7 for 32-bit Systems Service Pack 1
    - Windows 7 for x64-based Systems Service Pack 1
    - Windows Server 2008 for 32-bit Systems Service Pack 2
    - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
    - Windows Server 2008 for Itanium-Based Systems Service Pack 2
    - Windows Server 2008 for x64-based Systems Service Pack 2
    - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
    - Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
    - Windows Server 2008 R2 for x64-based Systems Service Pack 1
    - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Deny access to Remote Desktop Protocols (RDP) directly from the internet
  - Block all access to RDP, and
  - Utilise a VPN with multifactor authentication, if RDP is required
- Limit internal network machine to machine RDP
  - Apply appropriate internal network segmentation,
  - Deny standard workstations to arbitrarily connect to servers or other workstations over RDP (or any other unnecessary protocol), and
  - Limit RDP to servers; consider using a jump box to connect to other servers.
- Consider adding “Network Level Authentication” which adds a pre-exploitation hurdle. For more information on Microsoft’s Configuration of Network Level Authentication for Remote Desktop Services Connections, see here.

Detection

NCCGroup have developed a network detection rule that looks for potential signs of BlueKeep, pre-encryption.

For more information, see the github rules here.

References

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Github | NCCGroup network detection rules

Microsoft | Configuration for Network Level Authentication