CVE-2019-0708

Microsoft Remote Desktop Services (RDP)

Remote Code Execution Vulnerability (BlueKeep)

Purpose

As you would know, Microsoft recently disclosed the BlueKeep (CVE-2019-0708) vulnerability which targets the Remote Desktop Protocol (RDP) and is rated as a CRITICAL risk . BlueKeep impacts several versions of Windows including:

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

Microsoft has advised that RDP itself is not vulnerable and that this vulnerability is pre-authentication which requires no user interaction. On the 25th July 2019 it was revealed by ZDNet that a weaponised exploit was being sold commercially. This increased the likelihood of the exploit becoming publicly available.

Details

Through our contacts within the private and government sector Triskele Labs have been advised of an escalated level of preparedness for a public release of an exploit for this vulnerability in the coming days. Should this exploit become available to the general public, it will quickly spread and be utilised as a significant attack vector to the same scale as WannaCry. It is highly important all organisations are vigilant and ensure all vulnerable systems are patched and up to date. The Triskele Labs Advanced Security Operations Centre will also be checking with all clients that have configured vulnerability scanning assessments individually to confirm the mitigations have been actioned if scans have detected the vulnerability in their environments.

Mitigation Actions

Triskele Labs urges all IT teams to investigate their environments and confirm the below mitigating actions have been taken in their environments. To address CVE-2019-0708 patch the affected Windows operating systems with the patches listed below.

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

As an extra precaution, organisations are also advised to take the following additional mitigating steps

- Implement appropriate network segregation to restrict RDP to authorised subnets.
- Enable RDP access on an as needed basis.
- Never externally publish RDP. If required, utilise a Multifactor Authentication VPN
- Enable Network Level Authentication (NLA) on systems running vulnerable versions.

As always, the best precaution is to ensure all systems are patched and up to date.