Vulnerability Alert

Alert No: AVA190522 **Date: 22-May-19 13:31 PM**

Classification	**The Alert : Public Circulation Permitted**

Advisory Update: Microsoft RDP Vulnerability BlueKeep Criticality Update and Public Exploits Released

Overview	**Update on Advisory AVA190517: Microsoft Remote Desktop Protocol (RDP) vulnerability named BlueKeep criticality updated by Microsoft and has publicly available exploits.**
Description / Impact	The following vulnerability alert is an update to the alert AVA190517 published by FinCSIRT on the 17th of May 2019, related to the vulnerability advisory released by Microsoft on the 14th of May 2019, which detailed an exploit in the Remote Desktop Protocol has been updated by Microsoft. Successful exploitation of this vulnerability could allow an unauthenticated attacker to gain full user privileges on the exploited system and allow the attacker to install programs, view/change or delete data on affected systems. Microsoft has classified this vulnerability, now called "BlueKeep" as being a "wormable" exploit. This means that a malware exploiting this vulnerability can spread to other vulnerable machines without requiring user interactions without requiring user interactions, similar to the "WannaCry" vulnerability. This is officially acknowledged by the vendor and Microsoft has classified this vulnerability as 9.8 out of 10 making it a critical issue. Systems running Windows 10 and Windows 8 operating systems are not affected by this vulnerability.
Risk Reduction Recommendation	**Fix:** Microsoft has released updates for its currently supported operating systems: Windows 7, Windows Server 2008 R2, and Windows Server 2008. Microsoft has also released updates for its currently unsupported operating systems: Windows Server 2003 and Windows XP. It is recommended that external facing servers, with RDP enabled, be patched as soon as possible, followed by internal servers with RDP enabled and other internal workstations. **Note: In light of the system instability issues relating to the May 2019 update by Microsoft, it is recommended that the patch be tested before live deployment.** **Mitigation:** • Disable Remote Desktop Services if these are not being used/not business critical. **Workarounds:** • Enable Network Level Authentications on Windows 7, Windows Server 2008 and Windows Server 2008 R2 which support this feature. • Block RDB services (port 3389) on perimeter / enterprise firewalls to prevent attack from external parties.
Additional Information	**Visit the links below and follow the instructions given by respective vendors.** • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708 • https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708 • https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/
Disclaimer	The information provided herein is on "as is" basis, without warranty of any kind.