Title: Wormable BlueKeep Vulnerability

Introduction

On May 14, 2019, Microsoft has announced a new vulnerability that exists in older versions of Windows. The vulnerability could lead to new self-propagating malware that bears a striking resemblance to the infamous WannaCry that wreaked havoc on systems around the globe in 2017. The National Cyber Coordination and Command Centre (NC4) would like to advise all users of older version of Microsoft Windows to update your Windows by downloading and installing update as recommended by Microsoft to mitigate this issue.

Impact

Malicious code execution & Denial of Service

Brief Description

Microsoft has recently released a statement of a security flaw found in their older version of Windows operating systems, which enable attackers to remote code execute targets' machine. The vulnerability, which has been classified as CVE-2019-0708, is a remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability, which is called BlueKeep is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Based on alert from Microsoft, they are confident that an exploit exists for this vulnerability and nearly one million computers connected directly to the Internet are still vulnerable to CVE-2019-0708. Given the potential impact to customers and their businesses, Microsoft made the decision to make security updates available for affected platforms that are no longer in mainstream support. These updates are available from the Microsoft Update Catalog only. NC4 recommend that all users running one of these operating systems to download and install the update as soon as possible.

Affected Products

The following Microsoft Windows Operating Systems:

1. Windows XP SP3 x86;
2. Windows XP Professional x64 Edition SP2;
3. Windows XP Embedded SP3 x86;
4. Windows Server 2003 SP2 x86;
5. Windows Server 2003 x64 Edition SP2;
6. Windows 7 for 32-bit Systems Service Pack 1;
7. Windows 7 for x64-based Systems Service Pack 1;
8. Windows Server 2008 for 32-bit Systems Service Pack 2;
9. Windows Server 2008 for Itanium-Based Systems Service Pack 2;
10. Windows Server 2008 for x64-based Systems Service Pack 2;
11. Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1; and
12. Windows Server 2008 R2 for x64-based Systems Service Pack 1.

Recommendation

NC4 advises agencies to take the following actions:

1. Update all your Windows devices Operating Systems with the latest security patches (refer to customer guidance for CVE-2019-0708 links under Reference);
2. Block port 3389 (RDP) inbound and possibly outbound connection (if possible) until the patch is successfully installed; and
3. For any incidents related to this attack, please report to NC4.

Reference

1. CVE-2019-0708
   - https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
   - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
2. Dangerous New Vulnerability Forces Microsoft To Patch Windows XP Again https://www.forbes.com/sites/leemathews/2019/05/15/dangerous-new-vulnerability-forces-microsoft-to-patch-windows-xp-again/#2fbabcf156b1
3. Windows 7 and XP are vulnerable to a major security exploit -so patch now https://www.techradar.com/sg/news/windows-7-and-xp-are-vulnerable-to-a-major-security-exploit-so-patch-now
4. A Reminder to Update Your Systems to Prevent a Worm https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/
5. Almost One Million Vulnerable to BlueKeep Vuln CVE-2019-0708 https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XPSvoYgzbIU