DejaBlue: High Risk Windows Vulnerability
Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: Aug 15, 2019

## EXECUTIVE SUMMARY:

As a follow-up to our June 6, 2019 white paper on BlueKeep, this report documents a recent alert from Microsoft concerning two similar remote desktop protocol (RDP) vulnerabilities, entitled BlueKeep 2 and BlueKeep 3, together dubbed "DejaBlue." Researchers have identified about 800,000 devices that may be vulnerable, including systems running newer operating systems than were reported with BlueKeep, including Windows Server 2008 R2 Service Pack (SP) 1, 2012 and 2012 R2, Windows 7 Service Pack SP1, 8.1, and all versions of Windows 10. Windows versions not affected include Windows XP, and Server 2003 and 2008 (prior to R2). While these are not directly related to Bluekeep, similarly these vulnerabilities collectively pose significant risk to organizations and their data because of their exploit potential as attacks using the vulnerabilities could automatically spread from machine to machine.[i] Microsoft has released a patch for each vulnerability, and it is critically important for system administrators to scan and patch vulnerable systems as urgently as possible.[iii & iii]

## ANALYSIS:

As with BlueKeep and WannaCry Ransomware, the DejaBlue vulnerabilities are considered "wormable," meaning they can be spread rapidly and automatically – without user interaction – across the internet on unprotected systems. Therefore, malware that uses these vulnerabilities could affect hundreds of thousands of vulnerable systems, and then use other malware vectors and tactics to expose millions more that are not vulnerable.[i] Microsoft, who discovered the vulnerabilities on their own, quickly created patches, but has indicated that there has not been evidence of exploitation to date.[iii] Tactically, the solutions for mitigating the DejaBlue threat are very similar to those prescribed for BlueKeep; as described in the next section. Documented critical vulnerabilities include the two in question, CVE-2019-1181 and CVE2019-1182, and other important vulnerabilities CVE-2019-1223, CVE-2019-1224, and CVE-2019-1225.

The HPH sector is at risk from this vulnerability partially due to its wormable nature to Windows systems not already exposed to BlueKeep, as defined by the rapid spread of the wormable WannaCry Ransomware attacks, which crippled hundreds of thousands of systems across 150 countries.[ii] While with also-wormable BlueKeep, the HPH sector is vulnerable due to widespread use of legacy systems, including embedded systems in medical devices, the newer systems exposed to the DejaBlue vulnerabilities further extend and complicate the attack surface. It is fortunate that with newer systems, automated updates are potentially more-widely enabled, so more systems are likely to be patched immediately. However, due to the risk that automatic updates cause compatibility problems with older systems, not all IT infrastructures allow for automatic updating.

## PATCHES, MITIGATIONS, & WORKAROUNDS

Download and Apply the Patches: HERE[iii]

**Disable Remote Desktop Services if they are not required:** If organizations no longer need services (such as RDP) on the system, consider disabling them as a security best practice because disabling unused and unneeded services helps reduce organizations' exposure to security vulnerabilities.[iv]

**Enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2:** Organizations can enable Network Level Authentication (NLA) to block unauthenticated attackers from exploiting this vulnerability. With NLA turned on, an attacker would first need to authenticate to Remote Desktop Services using a valid account on the target system before the attacker could exploit the vulnerability.[iv]

**Block TCP port 3389 at the enterprise perimeter firewall**: TCP port 3389 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks. However, systems could still be vulnerable to attacks from within their enterprise perimeter.[iv]

**Determine if Remote Desktop Protocol (RDP) is enabled:** It is possible that users unknowingly and unnecessarily have RDP enabled. Individual users can perform a simple check to see if RDP is enabled on their computer. If RDP is enabled but not required, it is recommended to disable it by right-clicking on "My Computer" (Windows 10) / "This PC" (Windows 10) → selecting "Properties" → opening "Remote settings" tab → and selecting "Don't allow connections to this computer."[iv]

[i] David Caudery, "DejaBlue: New Bluekeep-Style Bugs Renew the Risk of a Windows Worm," 13 Aug 2019, accessed 15 Aug 2019; https://www.wired.com/story/dejablue-windows-bugs-worm-rdp/

[ii] Heather Landi, "Report: 40% of healthcare organizations hit by WannaCry in past 6 months," FierceHealthcare, 29 May 2019, accessed 5 Jun 2019; https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-month

[iii] "CVE-2019-1182 | Remote Desktop Services Remote Code Execution Vulnerability," 13 Aug 2019, accessed 15 Aug 2019; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182

[iv] Scott Caveza, "Tenable Roundup for Microsoft's August 2019 Patch Tuesday: DejaBlue," 13 Aug 2019, accessed 15 Aug 2019; https://www.tenable.com/blog/tenable-roundup-for-microsoft-s-august-2019-patch-tuesday-dejablue