LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF THE CHIEF INFORMATION OFFICER

HHS Healthcare Cybersecurity and Communications Integration Center (HCCIC)
Microsoft Vulnerabilities & Hidden Cobra 101 Report, June 15, 2017

Executive Summary:

Two reports were released by Microsoft and DHS this week about multiple vulnerabilities with Microsoft products, including the Windows operating system, and a threat by a group DHS labels as "Hidden Cobra". Both relate to the same type of vulnerability that allowed WannaCry to spread. Importantly, simply installing the Microsoft patches will not necessarily protect form "Hidden Cobra" since they use a wide range of vulnerabilities. DHS states "Hidden Cobra" targets are "…the media, aerospace, financial, and critical infrastructure sectors in the United States and globally", so targeting of the Healthcare and Public Health sector systems and devices in the U.S. is possible.

Business Impact:

These vulnerabilities allow an attacker to remotely run programs or attacks on systems. This could allow an attacker to perform a wide range of actions including exfiltrating documents or data, or gain access to other internal systems via the local network once initial access is gained.

Suggested Safeguards:

- Install the patches from Microsoft.
- Review the vulnerabilities in the US-CERT "Hidden Cobra" report and install associated patches.
- Review logs and implement blocks for indicators listed in the "Hidden Cobra" report.

Technical Information:

Microsoft released Security Advisory 4025685 highlighting vulnerabilities that were patched in the June release. The Advisory details several critical vulnerabilities in common Microsoft systems which must be patched immediately to prevent exploitation. Of note, CVE-2017-8543 is another vulnerability in the Server Message Block (SMB) protocol which was exploited in the WannaCry attack, and in this case can be remotely exploited via the Windows Search service. Exploitation of this type of SMB ("Server Message Block") vulnerability is frequently associated with foreign nation state cyber actors and is potentially extremely damaging to affected organizations.

SMB vulnerabilities can be extremely dangerous if left unpatched on a local (internal) corporate network. That's because a single piece of malware that exploits this SMB flaw within a network could be used to replicate itself to all vulnerable systems very quickly. The current SMB flaw, also affects older, unsupported versions of Windows such as Windows XP and Windows Server 2003. And, as with the previous SMB flaw, Microsoft has made the unusual decision to make fixes for this newer SMB bug available for those older versions

Another vulnerability which was patched could allow malicious code to spread quickly via shared drives. CVS-2017-8464 covers a vulnerability with how Windows handles the display of icons of shortcuts. Specially crafted shortcuts would allow vulnerable instances of Windows to execute the malicious code by simply viewing the link file without opening it.

Affected systems: Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012, Windows 8.1, Windows 8.1 RT, Windows Server 2012 R2, Windows 10, Windows Server 2016, Windows XP, Windows Vista, Windows 8, Windows Server 2003, and Windows Server 2003 R2