CYA 19-003

CONNECTICUT CYBER ALERT

1-866-HLS-TIPS

BlueKeep Exploit

28 May 2019

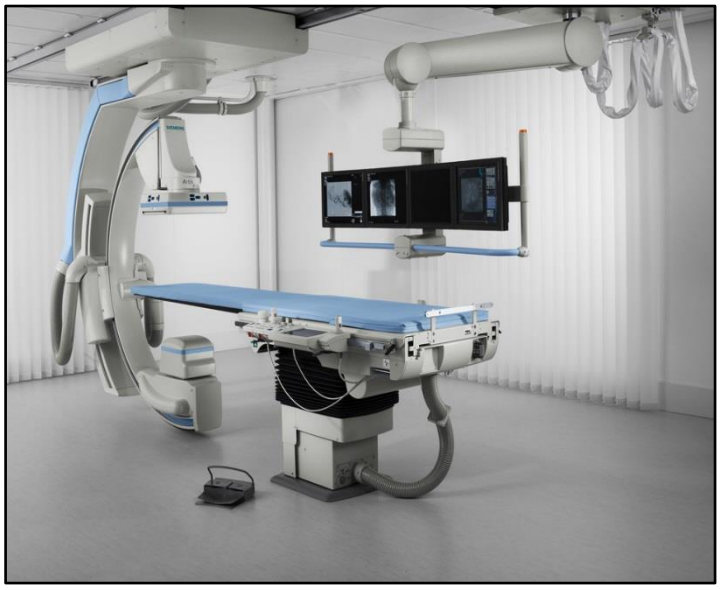
Scope Note

(U) The Connecticut Intelligence Center and the Cyber Crime Investigation Unit is providing this information for cyber situational awareness to public safety, emergency management, and private sector officials dealing with critical networks.

ALERT reporting should be considered unevaluated and is subject to modification.

ALERT NOTICE

(U) MESSAGE TYPE: **CTIC ALERT**



(U//TLP:WHITE) DETAILS/SITUATION: Microsoft recently issued a patch for an exploit named BlueKeep that uses specially crafted Remote Desktop Protocol (RDP) packets to gain system level privileges on a machine from a remote unauthenticated user. The exploit can be used on older windows operating systems such as Windows 7 and Windows Server 2008 and it is wormable, which means it can spread on its own. BlueKeep is similar in nature to the EternalBlue exploit that targeted unpatched machines to spread WannaCry in 2017 and thus there is the potential for another large scale attack that is similar in nature. Errata Security found that despite the patch being released two weeks ago there are still approximately 950,000 vulnerable devices connected to the internet. This past weekend threat actors began intensely scanning for vulnerable machines and we believe with a high level of confidence that there will be a cyber-attack utilizing this exploit in the near future.

(U//TLP:WHITE) Siemens has issued six security advisories regarding their medical equipment that is susceptible to this exploit. The affected devices include advanced therapy products, radiology and mobile X-ray products, laboratory diagnostic products, and radiation oncology products. There are a large number of vulnerable devices in the health care industry as one group, CyberMDX, proposed that BlueKeep currently affects around 70% of the medical devices in a typical hospital.

(U//TLP:WHITE) If these machines are compromised there could be life threatening consequences. Researchers in Israel published a paper in April were they were able to alter X-Ray images adding or removing cancer from patients scans with an extremely high success rate in tricking doctors. While that method has never been observed in the wild allowing an attacker to remotely execute code with system level privileges could lead to a large variety of other attacks that would negatively affect the health care industry. Based on this information we asses with moderate confidence that the health care industry is a potential target for this vulnerability in the near future and we believe that the potential damage from such an attack could be severe.

ATTENTION: Any attachments within this document might not be viewable from mobile devices. For best results, please utilize a PDF viewer from a desktop computer.

Please take a moment to complete this SURVEY and help evaluate the quality, value, and relevance of our product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. https://www.surveymonkey.com/r/CTIC_IM

For questions or comments, contact your Regional Intelligence Liaison Officer, or email CTIC at ctic@ct.gov
1111 Country Club Road Middletown CT, 06456 Telephone: (860) 706-5500

CONNECTICUT INTELLIGENCE CENTER

1111 Country Club Road,
Middletown, CT 06457

Email: ctic@ct.gov
Phone: (860) 706-5500

(U//TLP:WHITE) MITIGATION: In addition to updating all devices that are running older versions of Windows we recommend that inbound traffic on TCP port 3389 be blocked as well. The patches for the affected legacy operating systems can be downloaded from the following links.

- 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

(U) IMMEDIATE IMPACT ON CONNECTICUT: **YES**

(U) DISSEMINATION LIST: **Cyber All**

(U) CTIC and the Connecticut State Police Cyber Crime Investigation Unit will continue to monitor this reporting and will provide further information on the impact/significance to the State of Connecticut if warranted. Incident Reporting, Information and inquiries should be directed to CTIC at (860) 706-5500 or ctic@ct.gov. The Connecticut State Police Cyber Crime Investigation Unit can be reached at cybercrime@ct.gov or (860) 685-8450.

HSEC-6, HSEC-1