Title: CVE-2019-0708 Remote Desktop Protocol Vulnerability (Bluekeep & DejaBlue)
Advisory ID: CARESTREAM-2019-04
Issue Date: 05/16/2019
Last Revision Date: 06/04/2021
Revision #: 4

Vulnerability Summary:
On May 15, 2019, Microsoft released a fix for a critical Remote Code Execution vulnerability in Remote Desktop Services. This vulnerability was named Bluekeep. This vulnerability may be leveraged by a self-replicating worm to infect systems without any user interaction.

On August 13, 2019, Microsoft released several additional fixes for Remote Code Execution vulnerabilities in Remote Desktop Services. These vulnerabilities were named DejaBlue. These fixes build upon the previously released Remote Desktop Services patches from May 15 earlier in the year. These vulnerabilities may be leveraged by a self-replicating worm to infect systems without any user interaction.

Microsoft Remote Desktop Protocol vulnerabilities are currently being exploited by malicious actors. Steps should be taken to mitigate and/or patch these vulnerabilities.

CVE:

Bluekeep – Part 1 Vulnerabilities – May 15, 2019

ID	CVSS	Link	Impacted OS
CVE-2019-0708	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708	Windows XP, Vista, 7 Server 2000, 2003, 2008

Bluekeep – Part 2 Vulnerabilities – August 13, 2019

ID	CVSS	Link	Impacted OS
CVE-2019-1181	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1181	Windows XP, Vista, 7 Server 2000, 2003, 2008
CVE-2019-1182	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1182	
CVE-2019-1222	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1222	Windows 10, Server 2019
CVE-2019-1226	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1226	

Note that the original Bluekeep vulnerability did not impact Windows 8.1 / Windows Server 2012 and later. These new DejaBlue vulnerabilities impact all Windows Operating Systems.

Additional Information:

- https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve2019-1181-1182/
- https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
- https://www.zdnet.com/article/metasploit-team-releases-bluekeep-exploit/

©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021

Vulnerability Details:

These vulnerabilities are in the Remote Desktop Services component built into the Windows Operating System. Microsoft has determined that these are all critical (CVSS 3.0 Score 9.8) vulnerabilities. Therefore, Microsoft has additionally provided patches for the Windows XP and Windows Server 2003 Operating Systems even though they are no longer officially supported.

No user action is required to exploit this vulnerability. No credentials are required to connect to the Remote Desktop Service, and no privileges are needed. Therefore, these vulnerabilities could be leveraged by a self-replicating worm, similar to the WannaCry ransomware.

Mitigating the risk for the vulnerability:

Install the Bluekeep / DejaBlue patches that have been qualified for your system using the information below.

Additionally, Carestream recommends the following mitigations if Remote Desktop is not being used on the device:

- Disable incoming Remote Desktop connections via Control Panel -> System -> Remote Settings -> Don’t allow remote connections to this computer.
- Disable the Remote Desktop Services service through Control Panel -> Administrative Tools -> Services
- Block incoming connections to TCP Port 3389 (the Remote Desktop Protocol port) using a network or host-based firewall.

©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021

Affected Products and Patch Availability:

Impacted by Vulnerability	Product	Software Version	Operating System	Patch Availability
Impacted	CR825	DirectView V5.2 - V5.6	Windows XP Embedded SP3	Patch qualification for Bluekeep & DejaBlue vulnerabilities is complete. See below for more information.
	CR850			
	CR950			
	CR975	AND	AND	
	DIRECTVIEW Max CR System	DirectView V5.7	Windows Embedded Standard 7 SP1	
	DIRECTVIEW Classic CR System			
	DIRECTVIEW Elite CR System			
	DirectView Remote Operations Panel			
	DR 3000			
	DR 3500			
	DR 7500			
	DR 9500			
	DRX-Evolution			
	DRX-Evolution Plus			
	DRX-Ascend			
	DRX-Innovation			
	DRX-1 System			
	DRX-Revolution			
	DRX-Mobile Retrofit			
	Motion Mobile			
	DRX-Neo			
	DRX Mobile Upgrade Solutions			
	DRX-Transportable			
	DRX-Transportable Lite			
Impacted by DejaBlue Not Impacted by Bluekeep	OnSight 3D Extremity System	ImageView V1.1	Windows 10 1607 LTSB	Patch qualification for DejaBlue vulnerabilities is complete. See below for more information.

TMP-000377[A]
©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021

Impacted	DRX-Evolution DRX-Evolution Plus DRX-Ascend DRX-Innovation DRX-1 System DRX-Revolution DRX-Mobile Retrofit Motion Mobile DRX-Neo DRX Mobile Upgrade Solutions DRX-Transportable DRX-Transportable Lite	ImageView V1.2 +	Windows 10 1607 LTSB	Patch qualification for DejaBlue vulnerabilities is complete. See below for more information.
Not Impacted	DRX-Excel	Duet – All versions	Windows Embedded Standard 7 SP1	
Impacted	OMNI Products	All versions	Windows XP, 7	Customers may install the security updates on these devices. See below for more information.
Not Impacted	OMNI Products	All versions	Windows 8, 8.1	
Impacted	Image Suite Systems Crescendo Systems Vita Systems DRive	Image Suite – All versions	Windows XP, 7	Customers may install the security updates on these devices. See below for more information.
Impacted	Image Suite Crescendo Systems Vita Systems DRive	Image Suite – All versions	Windows 8, 8.1, 10	Customers may install the security updates on these devices. See below for more information.
Not Impacted	Tech Vision	All versions	Windows CE	Not network connected *
Not Impacted	Q-VISION	All versions	Windows	Not network connected *
Not Impacted	QV-800 Digital Universal System	All versions	Windows	Not network connected *
Not Impacted	ODYSSEY	All versions	Windows CE	Not network connected *
Not Impacted	QUEST	All versions	Windows CE	Not network connected *
Not Impacted	RAD-X Systems	All versions	Analog	

TMP-000377[A]

©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021

	Q-Rad			
Not Impacted	DRX Detectors	All models and versions	Linux	
Not Impacted	DRX Core Detectors	All models and versions	Linux	
Not Impacted	PRO Detector Systems	All models / versions	Linux	
Not Impacted	DV5700	All	Windows XPE	
Not Impacted	DV5700	1.9-2.0	WES2009	
Not Impacted	DV5950	All	Windows XPE	
Not Impacted	DV5950	1.8-2.0	WES2009	
Not Impacted	DV6950	All	Windows XPE	
Not Impacted	DV6950	1.5-2.0	WES2009	
Not Impacted	DV6800	1.0-2.08	Windows XPE	
Not Impacted	DV6800	2.09+	WES2009	
Not Impacted	DV6850	1.0-1.9	Windows XPE	
Not Impacted	DV6850	1.10+	WES2009	
Not Impacted	DV5800 / DV5850	All	Windows XPE	
Not Impacted	DV8900	All	Windows 2000	Mitigated by default configuration
Not Impacted	MyVue Center K2	All	WES7	
Not Impacted	MyVue Center K2	-	Windows 10	
Not Impacted	MyVue Center K3	All	WES7	
Not Impacted	MyVue Center K3	-	Windows 10	
Impacted	MyVue Center (Server)	All	Windows Server 2008	Patch qualification complete. See below for more information.
Not Impacted	Chroma	All	Windows XPE	

TMP-000377[A]
©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021

Patch Availability:

Product	Version(s)	Operating System	Patch Availability
DirectView	V5.2-V5.7	Windows XP & 7	Patch qualification complete. Contact your service provider for security updates or see: https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy for instructions on accessing the latest Security Roll-Up (SRU) tool on the Carestream service portal for self-installation.
ImageView	All versions	Windows 10 1607 LTSB	
Image Suite	All versions	Windows XP & 7	Customer may install the patch themselves via Windows Update or by downloading from Microsoft using the CVE links provided above.
OMNI	All versions	Windows XP & 7	
DB8900	All versions	Windows 2000	Microsoft Windows Server 2000 is confirmed vulnerable. A patch has not been made available by Microsoft. Customers should use network protections, blocking ports and other recommended mitigations above.
MyVue Center (Server)	All versions	Windows Server 2008	Contact your service provider for security updates.

To get Carestream's most secure medical device protections, Carestream recommends that customers stay current and upgrade to the latest version of software. Please contact your Carestream sales representative to inquire about updating.

Contact the Carestream Center of Excellence (COE) to coordinate patch installation or if you have additional questions. Service and support contacts can be found on Carestream's website at:
https://www.carestream.com/en/us/services-and-support

Remediation if infected with malware:
Customers who believe their systems are infected with malware should remove the device from the network and contact Carestream service or their service dealer for support.

Updates to this advisory:
Future updates to this advisory will be posted to Carestream's website:
https://www.carestream.com/en/us/services-and-support/cybersecurity-and-privacy

Note:
Carestream RIS, EIS, and PACS products are now managed by Philips after their purchase of Carestream Healthcare Information Systems. Please contact Philips for information regarding these products

©Carestream Health, Inc., 2019. CARESTREAM is a trademark of Carestream Health. 06/04/2021