Title: CVE-2019-0708 Remote Desktop Protocol Vulnerability (Bluekeep)
Advisory ID: CARESTREAM-2019-01
Issue Date: 05/16/2019
Last Revision Date: 06/21/2019
Revision #: 5

Vulnerability Summary:
On May 15, 2019, Microsoft released a fix for a critical Remote Code Execution vulnerability in Remote Desktop Services. This vulnerability may be leveraged by a self-replicating worm to infect systems without any user interaction. There are currently no known exploitations of this vulnerability.

CVE:

ID	CVSS 3.0 Score	Link
CVE-2019-0708	9.8	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

Additional Information:

- 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

Vulnerability Details:
This vulnerability is in the Remote Desktop Services component built into the Windows Operating System. This vulnerability impacts Windows XP, Windows Server 2000, Windows Server 2003, Windows Vista, Windows Server 2008 / 2008 R2, and Windows 7 Operating Systems. Windows 8.0/8.1 and Windows 10 are not impacted. Microsoft has determined that this is a critical (CVSS Score 9.8) vulnerability. Therefore, they have provided patches for the Windows XP and Windows Server 2003 Operating Systems even though they are no longer officially supported. Microsoft has not provided a patch for Windows Server 2000 operating systems.

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, this vulnerability could be leveraged by a self-replicating worm, similar to the WannaCry ransomware.

Mitigating the risk for the vulnerability:
DirectView and ImageView systems include a host-based Intrusion Prevention System (IPS) that uses a combination of whitelisting and sandboxing to prevent the infection off malware.

Carestream recommends the following guidance if Remote Desktop is not being used:

- 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.

Additional guidance specific to Carestream Imaging Systems products:

- For DirectView products, customers must wait for the qualified patch. The system doesn't allow customer installation of patches or alteration of the firewall. Other systems can be patched as indicated.
- For all Imaging Systems products, we do not use Remote Desktop and it may be disabled. DirectView / ImageView systems will not permit the user to do this at the host-based firewall.

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 complete for DirectView systems. *
	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			
Not Impacted	OnSight 3D Extremity System	ImageView V1.0	Windows 8.1 Industry Pro	
Not Impacted		ImageView V1.1	Windows 10 1607 LTSB	
Not Impacted	DRX-Revolution	ImageView V1.2	Windows 10 1607 LTSB	
Not Impacted	DRX-Excel	Duet – All versions	Windows Embedded Standard 7 SP1	
Impacted	OMNI Products	All versions	Windows XP, 7	Self-update *
Not Impacted	OMNI Products	All versions	Windows 8, 8.1	
Impacted	Image Suite Systems	Image Suite – All versions	Windows XP, 7	Self-update *
	Crescendo Systems			
	Vita Systems			
	DRive			
Not Impacted	Image Suite	Image Suite – All versions	Windows 8, 8.1, 10	
	Crescendo Systems			
	Vita Systems			
	DRive			
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 Q-Rad	All versions	Analog	
Not Impacted	DRX Detectors	All models and versions	Linux	Digital Detector *
Not Impacted	DRX Core Detectors	All models and versions	Linux	Digital Detector *
Not Impacted	PRO Detector Systems	All models / versions	Linux	Digital Detector *
Impacted	Directview PACS 5.2 and lower	All versions	WINDOWS 2003	Microsoft®

Impacted	Carestream PACS v10.x	All versions	WINDOWS 2003	Microsoft®
Impacted	Carestream PACS v11.x	All versions	WINDOWS 2008 R2	Microsoft®
Impacted	Vue RIS v11.0.x	All versions	WINDOWS 2003	Microsoft®
Impacted	Vue RIS v11.2.x	All versions	WINDOWS 2003	Microsoft®
Impacted	Carestream RIS v10.0.x & v10.1.x	All versions	WINDOWS 2003	Microsoft®
Impacted	EIS 3.1.x	All versions	WINDOWS 2003	Microsoft®
Impacted	EIS v3.1.x, v3.2 & v3.4	All versions	WINDOWS 2008 R2	Microsoft®
Impacted	Vue Cardio PACS v3.3	All versions	WINDOWS 2008 R2	Microsoft®
Not Impacted	Vue PACS v12.x and above	All versions	WINDOWS 2012 R2	
Not Impacted	Vue RIS v11.3 and above	All versions	WINDOWS 2012 R2	
Not Impacted	EIS v3.2 & v3.4	All versions	WINDOWS 2012 R2 WINDOWS 2016	
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	
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	Update to be provided
Not Impacted	Chroma	All	Windows XPE	

Patch qualification complete for DirectView systems. * - Please contact your service representative for installation or to obtain access to the Service Portal for customer download and self-installation.

Self-Update * – OMNI and Image Suite systems may be updated by the customer. The Microsoft patch may be obtained using the links provided above or via Windows Update.

Not network connected * – Tech Vision, Q-VISION, QV-800, ODYSSEY, QUEST, and RAD-X are standalone devices that do not connect to the customer network and are not impacted by this vulnerability.

Digital Detector * - These devices connect directly to an acquisition console and not the customer network.

Mitigated by default configuration.* - TCP port 3389 is disabled in the default configuration. Verify with local security team.

Microsoft® - Patches are available from Microsoft see the link in the table above.

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.

Patch Availability:

Product	Version(s)	Operating System	Patch Availability
DirectView	V5.2-V5.7	Windows XP & 7	Patch qualification complete. Please contact your service representative for installation or to obtain access to the Service Portal for customer download and self-installation.
Image Suite	All versions	Windows XP & 7	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
OMNI	All versions	Windows XP & 7	
Directview PACS 5.2 and lower	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
Carestream PACS v10.x	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
Carestream PACS v11.x	All versions	WINDOWS 2008 R2	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
Vue RIS v11.0.x	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
Vue RIS v11.2.x	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update

TMP-000377[A]

Carestream RIS v10.0.x & v10.1.x	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
EIS 3.1.x	All versions	WINDOWS 2003	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
EIS v3.1.x, v3.2 & v3.4	All versions	WINDOWS 2008 R2	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
Vue Cardio PACS v3.3	All versions	WINDOWS 2008 R2	Customer may install the patch themselves by downloading from Microsoft or via Windows Update
DV8900	All	Windows 2000	Microsoft Windows Server 2000 is confirmed vulnerable. Customers should use network protections, blocking ports and other recommended mitigations.
MyVue Center (Server)	All	Windows Server 2008	Update to be provided

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

Microsoft Windows Server 2000 is confirmed vulnerable. Customers should use network protections, blocking ports and other recommended mitigations. Microsoft has not provided a patch for Windows Server 2000 operating systems.

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