Title: Remote Desktop Protocol Vulnerability (Bluekeep – Part 2)
Advisory ID: CARESTREAM-2019-03
Issue Date: 08/15/2019
Last Revision Date: 10/28/2019
Revision #: 3

Vulnerability Summary:
On August 13, 2019, Microsoft released several fixes for Remote Code Execution vulnerabilities in Remote Desktop Services. 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.

9/9/19 Update: Researchers at Metasploit released an exploit for this vulnerability. It should be noted that the exploit requires user interaction to execute correctly, and it only works against 64-bit versions of Windows 7 and Windows 2008 R2, but not other Windows versions that are vulnerable to BlueKeep.

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 7, 8.1, 10, Svr 2008, 2012, 2016, 2019
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 Bluekeep vulnerabilities impact all Windows Operating Systems.

Additional Information:

- https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
- https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
- https://www.zdnet.com/article/metasploit-team-releases-bluekeep-exploit/

Vulnerability Details:

These vulnerabilities are in the Remote Desktop Services component built into the Windows Operating System. They impact Windows XP / Windows Server 2000 and later Operating Systems. Microsoft has determined that these are all critical (CVSS 3.0 Score 9.8) vulnerabilities. Therefore, Microsoft has 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, these vulnerabilities could be leveraged by a self-replicating worm, similar to the WannaCry ransomware.

Mitigating the risk for the vulnerability:

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 (X-Ray Capture) products:

- DirectView and ImageView systems include a host-based Intrusion Prevention System (IPS) that uses a combination of whitelisting and sandboxing to prevent the infection of malware.
- For all Imaging Systems products, Remote Desktop is not used and should already be disabled by default. Remote Desktop is not used by service for remote access connectivity. Disabling the Remote Desktop service will have no impact on these systems. These patches are being qualified for these systems as a precautionary measure.
- For DirectView products, patches for Bluekeep Part 1 have been validated and made available. For Bluekeep Part 2 patches, DirectView customers must wait for the qualified patch. DirectView systems do not allow customer installation of unqualified patches or alteration of the firewall. Other systems can be patched as indicated.
- ImageView products run Windows 8.1 and 10 Operating Systems and were not impacted by the Bluekeep Part 1 vulnerability. Patches are currently being qualified for Bluekeep Part 2.

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 Bluekeep Part 1 Vulnerabilies. *
	CR850			
	CR950			
	CR975	AND	AND	
	DIRECTVIEW Max CR System	DirectView V5.7	Windows Embedded Standard 7 SP1	Patch qualification complete for Bluekeep Part 2 Vulnerabilities.
	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 Impacted Not Impacted	OnSight 3D Extremity System DRX-Revolution All products	ImageView V1.1 ImageView V1.2 ImageView V1.3 +	Windows 10 1607 LTSB	Patch qualification in progress for Bluekeep Part 2 Vulnerabilities.
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 Crescendo Systems Vita Systems DRive	Image Suite – Version 4 MR4 or earlier.	Windows XP, 7, 8, 8.1, 10	Self-update *
Impacted	Image Suite Crescendo Systems Vita Systems DRive	Image Suite – Version 4 MR5 or later.	Windows 8.1, 10	Customers should upgrade to V4 MR7 or later. Patch qualification in progress for Bluekeep Part 2 Vulnerabilities.
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 *
Not Impacted	DV5700	All	Windows XPE	
Not Impacted	DV5700	1.9-2.0	WES2009	
Not Impacted	DV5950	All	Windows XPE	

TMP-000377[A]

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 for the Bluekeep Part 1 vulnerability is 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.

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 is complete for the Bluekeep Part 1 vulnerability. Please contact your service representative for installation or to obtain access to the Service Portal for customer download and self-installation. • Patch qualification is complete for the Bluekeep Part 2 vulnerability.
ImageView	V1.1 - V1.2	Windows 10 1607 LTSB	• Not impacted by the Bluekeep Part 1 vulnerability. • Patch qualification for the Bluekeep Part 2 vulnerability is in progress.
ImageView	V1.3+	Windows 10 1607 LTSB	• Not impacted by the Bluekeep Part 1 vulnerability. • Patch qualification for the Bluekeep Part 2 vulnerability is in progress.
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	
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

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.