Title:	**Carestream Product Security Advisory – July 2023**
Advisory ID:	CARESTREAM-2023-01
Issue Date:	08/16/2023
Last Revision Date:	08/16/2023
Revision #:	1

Vulnerability Summary:

A series of MSMQ, RPC, ICMP, and HTTP vulnerabilities were addressed by Microsoft in 2023 that may impact some Carestream products.

To address these issues, Carestream has qualified and made available the latest July 2023 security updates which incorporate the fixes for July and previous months.

CVE(s):

ID	CVSS	Link
CVE-2023-32057	9.8	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057
CVE-2023-23392	9.8	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23392
CVE-2023-23415	9.8	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23415
CVE-2023-24908	8.1	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24908
CVE-2023-24869	8.1	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24869
CVE-2023-23405	8.1	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23405
CVE-2023-21708	9.8	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21708

Affected Products and Patch Availability:

The following systems are impacted by these vulnerabilities with available security updates:

- Wave Injection System 1.0
- Image Suite systems running on Windows 10 or Windows 11 Version 21H2 and later.

Perform the following steps to apply the Microsoft July 2023 security updates which addresses the above CVEs.

Wave Injection System

- Engage Carestream service to install Wave Injection System software version 1.1 which is available at the end of August 2023.

Image Suite systems

- Before applying the security updates, you must first execute a Carestream script to configure the Microsoft Update services to the correct settings.
  Note: This step needs to be completed once. If this has already been done as part of a previous vulnerability remediation, then you may skip this step. There is no harm in performing this step a second time.
  To configure the Microsoft Update services:
  - Contact Carestream service and request Cyber Security End User Group Access to the Service Portal. For service contact information, see: https://www.carestream.com/en/us/services-and-support/world-wide-contacts
  - After receiving your credentials, you may logon to the Service Portal: https://serviceportal.carestreamhealth.com/
  - Navigate to Service Assets → Choose Products: Image Suite Cybersecurity
  - Download InstallWsusSetupUtility.zip and extract the contents of the zip file.
  - In the newly extracted folder, go to InstallWsusSetupUtility and run InstallWsusSetup.bat as an Administrator.
  - Reboot the Image Suite system.
- Image Suite customers may now apply patches directly from Microsoft.
  - Download and install the correct January 2022 roll-up for your system:

Windows OS	Patch	Link
Win11 21H2	KB5028182	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5028182
Win11 22H2	kb5028185	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5028185
Win10 21H2	kb5028166	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5028166
Win10 22H2	kb5028166	https://www.catalog.update.microsoft.com/Search.aspx?q=KB5028166

Complete list of Carestream Products and Impact Status:

Impacted by Vulnerability	Product	Patch Availability
ImageView V2.0 & later Systems – Windows 10 IoT Enterprise 2021 LTSC		
Not applicable to device	DRX-Evolution	None
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Rise	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.8-1.11 Systems – Windows 10 IoT Enterprise 2019 LTSC		
Not applicable to device	DRX-Evolution	None
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Rise	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.2-1.7 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Not applicable to device	DRX-Evolution	None
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	

Impacted by Vulnerability	Product	Patch Availability
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.1 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Not applicable to device	OnSight 3D Extremity System	None
DirectView V5.7 Systems – Windows Embedded Standard 7 Service Pack 1		
Not applicable to device	CR975	None
	DIRECTVIEW Max CR System	
	DIRECTVIEW Classic CR System	
	DIRECTVIEW Elite CR System	
	DirectView Remote Operations Panel	
	DRX-Evolution	
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
DirectView V5.2 – V5.6 Systems – Windows XP Embedded Service Pack 3		
Not applicable to device	CR825	None
	CR850	
	CR950	
	CR975	
	DIRECTVIEW Max CR System	
	DIRECTVIEW Classic CR System	
	DIRECTVIEW Elite CR System	
	DIRECTVIEW Remote Operations Panel	
	DR 3000	
	DR 3500	

Impacted by Vulnerability	Product	Patch Availability
	DR 7500	
	DR 9500	
	DRX-Evolution	
	DRX-Ascend	
	DRX-Innovation	
	Q-Rad Systems	
	DRX-1 System	
	DRX-Revolution	
	DRX-Mobile Retrofit	
	DRX-Neo	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
Image Suite V4 Systems – Windows 10 Professional		
Patch available for Windows 10 and Windows 11 21H2 and later	CRescendo Classic Image Suite	Microsoft patches have been qualified any may be installed. See above for more information.
	CRescendo WAIV Series with Touch Screen	
	CRescendo Vita Image Suite	
	CRescendo Max	
	Vita CR System	
	Vita Flex CR System	
	DRive	
	PRO Detector Systems	
Image Suite V4 Systems – Windows 8.1 Professional		
Not applicable to device	CRescendo Classic Image Suite	None
	CRescendo WAIV Series with Touch Screen	
	CRescendo Vita Image Suite	
	CRescendo Max	
	Vita CR System	
	Vita Flex CR System	
	DRive	
	PRO Detector Systems	
Duet Version 1.0 – 1.13 – Windows Embedded Standard 7 Service Pack 1		
Not applicable to device	DRX-Excel	None
	DRX-Excel Plus	
Duet Version 1.20 – Windows 10 IoT Enterprise 2016 LTSB		
Not applicable to device	DRX-Excel	None
	DRX-Excel Plus	

Impacted by Vulnerability	Product	Patch Availability
OMNI Products		
Not applicable to device	OMNI	None
Wave Injection System – Windows 10 IoT Enterprise 2021 LTSC		
Patch available for Version 1.0	Wave Injection System	Microsoft patches have been qualified any incorporated into the next release of software. See above for more information.
X-Ray Detectors		
Not applicable to device	DRX Detectors	None
	DRX 2530C Detector	
	DRX Plus Detectors	
	DRX Plus 2530C Detector	
	DRX Core Detectors	
	PRO Detectors	
	DRX-L Detector	
	Focus Detectors	
Analog Systems / Not network connected		
Not applicable to device	QV-800 Digital Universal System	None
	Q-VISION	
	RAD-X Systems	
	Motion Mobile	
	ODYSSEY	
	QUEST	
	Tech Vision	
DryView – Windows XP Embedded Service Pack 3		
Not applicable to device	DRYVIEW 5700	None
	DRYVIEW 5950	
	DRYVIEW 6950	
DryView – Tux Linux		
Not applicable to device	DRYVIEW 5700	None
	DRYVIEW 5950	
	DRYVIEW 6950	
MyVue Kiosk Terminal		
Windows 10	Kiosk K3 Kiosk K5	None
MyVue Kiosk Print Server		
Windows Server 2016	Kiosk Print Server	None

Impacted by Vulnerability	Product	Patch Availability
Windows Server 2022	Kiosk Print Server	None
INDUSTREX Non-Destructive Testing – Detectors		
Not applicable to device	HPX-DR 3543 PE Detector	None
	HPX-DR 4336 GH Detector	
	HPX-DR 2530 GH Detector	
	HPX-DR 2530 GC Detector	
	Exposure Interface Box (EIB)	
INDUSTREX Non-Destructive Testing – CR Systems		
Not applicable to device	HPX-PRO Portable Digital System	None
	HPX-1 Digital System	
	HPX-1 Plus Digital System	
INDUSTREX Non-Destructive Testing – Software		
	Digital Viewing Software	None
	ayData NDT Archive	
INDUSTREX Non-Destructive Testing – Processors		
Not applicable to device	M43ic Processor	None
	M37 Plus Processor	

Vulnerability Details:
Please see the CVE links above for CVE details.

Mitigating the risk for the vulnerability:
Blocking impacted network ports such using a software or hardware firewall will prevent remote access to impacted Windows services.

Protocol	Port
HTTP(S)	TCP: 80, 443
MSMQ	TCP & UDP: 1801
RPC	TCP: 135, 2101, 2103, 2105

Patch Availability:

Product	Version(s)	Patch Availability
Image Suite	V4.0	Microsoft patches have been validated. See above for more information.
Wave Injection System	V1.0	Microsoft patches have been validated. See above for more information.

Please contact your Carestream sales representative to inquire about updating to the latest version of software.

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

Carestream Product Security Guidance:
Carestream continuously evaluates the cybersecurity strategy of its products and often includes security patches and improvements with each software release. In order to maximize the resilience of your equipment, Carestream recommends customers keep their devices current by upgrading to the latest software release available for the product(s).
Carestream strongly recommends customers apply a layered security approach to protect all of their medical devices including Carestream equipment. Recommendations include but are not limited to:

- **Updates:** Apply software and security updates to the medical device when available.
- **Encryption:** Leverage Data at Rest and Data in Transit solutions to protect confidential data and the security of the system.
- **Physical Security:** Physically limit access to equipment when possible.
- **Role Based User Access**: Limit access to the equipment to authorized users only and minimize user privileges by role.
- **Network Isolation and Segmentation:** Firewalls, network segmentation, and/or virtual LANs should be used and configured to limit network communication of medical devices to only the addresses and ports required to support your workflow.

- **Endpoint & Network Monitoring:** Monitor the actions of devices at the endpoint and on the network through firewall, intrusion detection, endpoint audit logs by forwarding these logs to a Security Information and Event Management (SIEM) system.
- **Intended Use:** Only use Carestream products for intended use – do not check personal email, browse the internet, or install applications not required for the medical device

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