Title: Heap Overflow vulnerability in Google Chrome / Microsoft Edge
Advisory ID: CARESTREAM-2021-01
Issue Date: 02/22/2021
Last Revision Date: 03/02/2021
Revision #: 2

Vulnerability Summary:

CVE-2021-21148 is a heap buffer overflow vulnerability in V8, Google Chrome's open-source JavaScript and Web Assembly engine. This vulnerability allows a remote attacker to potentially exploit heap corruption via a crafted HTML page. This affects Google Chrome browsers with versions < 88.0.4324.15 and Microsoft Edge browsers with versions < 88.0.705.63.

CVE(s):

ID	CVSS 3.0 Score	Link
CVE-2021-21148	8.8 High	CVE - CVE-2021-21148 (mitre.org)

Additional Information:

- CVE - CVE-2021-21148 (mitre.org)
- Google patches an actively exploited Chrome zero-day | ZDNet
- Google Chrome update patches this major security issue | TechRadar

Affected Products and Patch Availability:

Impacted by Vulnerability	Product	Patch Availability
ImageView V1.8-1.X Systems – Windows 10 IoT Enterprise 2019 LTSC		
Mitigated by compensating control *	DRX-Evolution	Chrome to be updated with next software release.
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	

Impacted by Vulnerability	Product	Patch Availability
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.3-1.7 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Mitigated by compensating control *	DRX-Evolution	Chrome to be updated with next software release.
	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	
ImageView V1.1 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Mitigated by compensating control **	OnSight 3D Extremity System	None
DirectView V5.7 Systems – Windows Embedded Standard 7 Service Pack 1		
Not Impacted	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	

Impacted by Vulnerability	Product	Patch Availability
	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 Impacted	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	
	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		
Not Impacted ***	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	

Impacted by Vulnerability	Product	Patch Availability
	PRO Detector Systems	
Image Suite V4 Systems – Windows 8.1 Professional		
Not Impacted ***	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 Impacted	DRX-Excel	None
	DRX-Excel Plus	
Duet Version 1.20 – Windows 10 IoT Enterprise 2016 LTSB		
Not Impacted	DRX-Excel	None
	DRX-Excel Plus	
OMNI Products		
Impacted****	OMNI	None
X-Ray Detectors		
Not Impacted	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 Impacted	QV-800 Digital Universal System	None
	Q-VISION	
	RAD-X Systems	
	Motion Mobile	
	ODYSSEY	
	QUEST	

Impacted by Vulnerability	Product	Patch Availability
	Tech Vision	
DryView – Windows XP Embedded Service Pack 3		
Not Impacted	DRYVIEW 5700	None
	DRYVIEW 5950	
	DRYVIEW 6950	
DryView – Tux Linux		
Not Impacted	DRYVIEW 5700	None
	DRYVIEW 5950	
	DRYVIEW 6950	
MyVue – Windows 10		
Mitigated by compensating control**	MyVue Center K3 Kiosk	None
MyVue – Windows Server 2016		
Mitigated by compensating control**	MyVue Center K3 Kiosk	None

* ImageView 1.3 – 1.8 has a browser web proxy feature that prevents browsing to any websites except Microsoft and Carestream.

** No access to desktop or browser for end-users.

*** Edge and Chrome are not components of the ImageSuite software product. Carestream recommends this and other 3rd party components present on the medical device be kept up to date by following the guidelines provided by the vendor of that software. Also, please reference the Carestream Product Security Guidance below for intended use of the medical device.

**** Omni products auto update OS and browser. Customer can auto update using Windows update.

Vulnerability Details:

For this vulnerability to be exploited, a user must use one of the affected browsers and navigate to a specially crafted URL. These malicious URL's would typically be included in a phishing email. Please see Carestream guidance below to limit risk.

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:

An updated version of this advisory will be published by March 1st, 2021.

https://www.carestream.com/services-and-support/cybersecurity-and-privacy