Title: **Support for Windows Embedded Standard 7 SP1 ends 10/13/2020**
Advisory ID: CARESTREAM-2020-04
Issue Date: 9/8/2020
Last Revision Date: 10/6/2020
CVE(s):

Advisory:
Microsoft announced the "End of Life" for Windows Embedded Standard 7 SP1 will be October 13, 2020. Patches will not be available to address cybersecurity vulnerabilities for the Windows Embedded Standard 7 SP1 operating system. This may leave certain Carestream products vulnerable to exploitation by malicious actors.

Are Carestream Products affected?
Yes, affected products are detailed in table 1 below.

How can I mitigate the risk to my equipment / data?
The recommended strategy to protect your equipment is to upgrade to the latest version of Carestream software, ImageView. In the event that ImageView is not available for your product, the Microsoft Extended Security Updates program may be available.

Please contact your Carestream sales, service sales, or field service representative to coordinate an upgrade to the ImageView platform (recommended) or enroll in the Microsoft Extended Security Updates program, or if you have additional questions.

Table 1:

Carestream Product	Product Software	Path to Protection
DRX-Evolution/Evolution Plus	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
DRX-1 Systems	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
DRX-Ascend / Q-Rad	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
DRX-Revolution / Revolution Nano	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
DRX-Mobile Retrofit / DRX Mobile Upgrade Solutions (except Siemens configuration)	DirectView 5.7 (Windows 7 embedded)	Extended Security Updates / Upgrade from DirectView to ImageView* (Windows 10 IoT)
DRX-Transportable / Transportable Lite	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView* (Windows 10 IoT)
CR Classic	DirectView 5.7 (Windows 7 embedded)	Extended Security Updates
CR Elite	DirectView 5.7 (Windows 7 embedded)	Extended Security Updates
Nano	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
CR Max/CR975	DirectView 5.7 (Windows 7 embedded)	Extended Security Updates / Replace with Ascend
Q-Vision	DirectView 5.7 (Windows 7 embedded)	Upgrade from DirectView to ImageView (Windows 10 IoT)
Caresteam products running versions of DirectView older than 5.7 DRX-Evolution System, DRX-1, DR 5000, DR5100, DR7100, DR7500, DR9000, DR9500, DR3500, DR3000,	Windows 2000 / Windows XP Embedded SP3	Contact your sales representative for upgrade options

Classic and Elite CR Systems, CR500, CR800, CR825, CR850, CR900 CR950, CR975, ROP, DRX Mobile Retrofit, Classic, Elite and Max CR Systems, DirectView Remote Operations Panel		
Kiosk K2 / K3	Windows 7 embedded	Upgrade to Windows 10

* solution may be region dependent

Carestream Guidance:

Carestream continuously evaluates the cybersecurity strategy of its products and as such often includes security patches and improvements with each software release. In order to maximize the resilience of your equipment, Carestream recommends customers keep their device's 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:

• **Physical Security**—Physically limit access to equipment when possible.

• **Role Based User Access**—Limit access to the equipment to authorized users only and minimizing 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.

• **Network Monitoring**—Monitor the actions of devices on the network through firewall, intrusion detection, and SIEM (Security Information and Event Management) logs