Title: **Meltdown and Spectre Vulnerabilities**
Advisory ID: CARESTREAM-XRS-2018-01
Issue Date: 01/05/2018
Last Revision Date: 01/18/2018

Vulnerability Summary:
This advisory addresses the "speculative execution side-channel attacks" known as ***Meltdown*** and ***Spectre***.

Meltdown is a hardware vulnerability found in Intel and other computer processors. It allows a malicious program to read the memory of other processes and the kernel.

Spectre refers to a class of vulnerabilities that exploit the branch prediction feature of modern processors. A malicious program can trick the processor into assuming that a given instruction will execute in the future and pre-load the necessary memory to support that instruction. This allows a malicious program to read memory it should not have access to.

Currently there are no known exploits that leverage the ***Meltdown*** or ***Spectre*** vulnerabilities, and there are no known instances of Carestream equipment being impacted. The Microsoft Advisory for these vulnerabilities has been classified as Important. Malicious software must already be running on the machine in order to exploit these information disclosure vulnerabilities.

CVE(s):

ID	CVSS 3.0 Score	Link
CVE-2017-5754	5.6 Medium	https://nvd.nist.gov/vuln/detail/CVE-2017-5754
CVE-2017-5753	5.6 Medium	https://nvd.nist.gov/vuln/detail/CVE-2017-5753
CVE-2017-5715	5.6 Medium	https://nvd.nist.gov/vuln/detail/CVE-2017-5715

Additional Information:

- Microsoft Advisory on ***Meltdown*** and ***Spectre***
  - ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
- Windows Client Guidance for IT Pros to protect against speculative execution side-channel vulnerabilities
  - https://support.microsoft.com/en-us/help/4073119/
- Intel Issues Updates to Protect Systems from Security Exploits
  - https://newsroom.intel.com/news-releases/intel-issues-updates-protect-systems-security-exploits/

Microsoft has made patches available for Windows 7, 8.1 and 10 Operating Systems.
Windows XP and 8 are no longer supported by Microsoft.

Affected Products:

The Microsoft patch is currently being evaluated for the following products:

Impacted by Vulnerability	Product	Software Version	Operating System
Yes	DIRECTVIEW Max CR System / DR975	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DIRECTVIEW Classic CR System	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DIRECTVIEW Elite CR System	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DIRECTVIEW Remote Operations Panel	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Evolution	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Evolution Plus	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Ascend	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-1 System	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Revolution	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Mobile Retrofit	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX Mobile Upgrade Solutions	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Transportable	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	DRX-Transportable Lite	DirectView V5.7	Windows Embedded Standard 7 SP1
Yes	OnSight 3D Extremity System	ImageView V1.0	Windows 8.1 Industry Pro

For Carestream products running Image Suite software, Carestream Pro Detector Systems, and OMNI Products, we recommend customers manually run Window Update on your systems to ensure you have the most up-to-date security patches from Microsoft

For all other products or versions not explicitly not mentioned here a patch will **not** be made available. As a precaution, we recommend customers assume these systems are vulnerable and only use the equipment for its intended purpose. The system must load and run malicious software to exploit this vulnerability.

You can also talk to your Carestream sales representative to discuss equipment trade-in / trade-up options for new systems.

Vulnerability Details

Meltdown and ***Spectre*** are information disclosure vulnerabilities. Each would require a user to load and activate a malicious process or program leveraging the exploits to gain access to unauthorized information. This could be done by browsing to a malicious website or loading and executing a program from a USB drive.

Carestream DirectView, ImageView, and Ultrasound products do not allow the local operator to browse websites or execute software from USB drives. Carestream DirectView and ImageView products also include Symantec

Critical System Protection (SCSP) – a host-based Intrusion Prevention System that will prevent unknown software from executing.

For other systems, it is recommended that the equipment only be used for its intended purpose. Do not browse the internet or install and run 3rd party applications on the device.

Please contact your Carestream sales, service sales, or field service if you have additional questions.

Mitigating the risk for the vulnerability

It is suggested that the medical device be only used for its intended purpose. Browsing the internet, reading emails, downloading files, installing 3rd party software via USB, … can all expose the system to malicious software.

These vulnerabilities require malicious software to already be running on the medical device, so there are no network firewall or other mitigations that can be applied to mitigate the risk.

Remediation if infected with malware

There are currently no known exploits leveraging the ***Meltdown*** or ***Spectre*** vulnerabilities. If you believe your system has become infected with any type of malware, please contact the Carestream Center of Excellence (COE).

Anti-Virus

Most Anti-Virus software has been updated to detect and prevent malicious software from exploiting these vulnerabilities.

- DirectView & ImageView: These systems use Symantec Critical System Projection (SCSP) as a critical aspect of their overall security scheme. SCSP uses heuristic analysis and white-listing to prevent unauthorized software from executing.
    - Carestream does not allow the installation of unverified software which includes Anti-Virus software. Carestream performs extensive verification and validation testing on its products in their delivered configurations to ensure their safe and effective operation. Installation of 3rd party Anti-Virus software is not permitted.
- ImageSuite: Third party Anti-Virus may be installed on ImageSuite systems.

Patch Availability

- DirectView & ImageView: Carestream is evaluating and testing the Microsoft patches for DirectView and ImageView systems running supported versions of the Microsoft OS. Patches are expected to be available for installation on or before February 12, 2018.
- ImageSuite: Microsoft patches may be installed directly through Windows Update.

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

Contact the Carestream Center of Excellence (COE) if you have additional questions or to coordinate patch installation. Service and support contacts can be found on Carestream's website at:

https://www.carestream.com/en/us/services-and-support

Updates to this advisory

Future updates to this advisory will be posted to Carestream's website at:

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