Security Advisory

Overview:

Note: This Vulnerability Note is the product of ongoing analysis and represents our best knowledge as of the most recent revision. As a result, the content is subject to change as further analysis is performed and the results are updated.

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre. Both Spectre and Meltdown take advantage of the ability to extract information by executing instructions on a CPU using the CPU cache/system memory as a side-channel. These attacks are described in detail by Google Project Zero, the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz) and Anders Fogh.
(**CERT REF:** http://www.kb.cert.org/vuls/id/584653)

In order that an attacker to access the CPU cache/system memory, the attacker must be able to first run malicious code on the device. As a general scenario for executing malicious code, the followings are well-known.

- Accessing the Internet using a Web browser and execute a script
- Opening a file attached to an e-mail
- The autorun function to execute a program on a device such as a USB memory

On the medical device, various security controls to deter the malicious code execution are implemented. Those security controls do not readily provide a way for attackers to execute malicious code locally and therefore face significantly lower risk.
Canon Medical Systems Corporation (CMSC) manufacture knows that patches are being provided from the manufacturer of CPU and OS and understands the risk of side effects such as performance degradation and blue screen. In the present circumstances, CMSC recognizes that the risk of side effects is more problematic than the possibility of information leakage. CMSC will continue to monitor this vulnerability for further information as it is provided.

Overview description: https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
Detailed description: https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life

Security Advisory

Possible Affected CMSC Products (investigating):

- All diagnostic imaging equipment

Unaffected Products (investigating)

- Under Investigation

Resolution

CMSC will continue to monitor this vulnerability for further information as it is provided.

Notes:

Continue to check this advisory for updated information. Please email CanonMedicalSystemsSecurity@us.medicalcanon with any specific questions or issues.

Vulnerability Information

- CVE-2017-5753,Spectre: Bounds check bypass
- CVE-2017-5715,Spectre: Branch target injection
- CVE-2017-5754, Meltdown: Rogue data cache load, memory access permission check performed after kernel memory read

Advisory Change Log

This is the second release of this Advisory

Release Date: 01/15/2018

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life