Security Advisory

Revised Release Date: September 6th, 2019

URGENT/11 WindRiver VXWorks

Overview

CVE-2019-12256 | Stack overflow in the parsing of IPv4 options

REF:

- https://nvd.nist.gov/vuln/detail/CVE-2019-12256

CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, CVE-2019-12263 | Memory corruption vulnerabilities stemming from erroneous handling of TCP's Urgent Pointer field

REF:

- https://nvd.nist.gov/vuln/detail/CVE-2019-12255
- https://nvd.nist.gov/vuln/detail/CVE-2019-12260
- https://nvd.nist.gov/vuln/detail/CVE-2019-12261
- https://nvd.nist.gov/vuln/detail/CVE-2019-12263

CVE-2019-12257 | Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc

REF:

- https://nvd.nist.gov/vuln/detail/CVE-2019-12257

Affected Versions: VxWorks versions 6.9.4.11, Vx7 SR540 and Vx7 SR610

URGENT/11 is a set of 11 vulnerabilities found to affect VxWorks' TCP/IP stack (IPnet), used by the versions of VxWorks as described above. Six of the vulnerabilities are classified as critical and enable Remote Code Execution (RCE). The remaining vulnerabilities are classified as denial of service, information leaks or logical flaws. As each vulnerability affects a different part of the network stack, it impacts a different set of VxWorks versions.

REF:

- https://www.armis.com/urgent11/

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

Notes:

This Vulnerability Advisory 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.

Canon Medical Systems Corporation has completed the applicability of this vulnerability to Medical Imaging Devices manufactured by Canon Medical Systems Corporation.

Canon Medical Systems USA, Inc. has completed the investigation of the applicability of the vulnerability to InnerVision products.

The products below are using VXWorks V6.5 and above, however there is no risk to these systems. The implementation of VXWorks on these systems are used internally and are not connected, or part of the network boundary, to the healthcare facilities TCP/IP network. Therefore with no threat, there is no risk.

Vascular (VL): Infinix systems V6.9 and higher

Computed Tomography (CT):

• Aquilion LB	TSX-021A/3
• Alexion	TSX-032A
• Alexion	TSX-034A
• Aquilion Lightning	TSX-035A
• Aquilion Start	TSX-037A

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

Made For life

Affected Canon Medical Systems Products:

No products manufactured by Canon Medical Systems Corporation are impacted

No InnerVision products are impacted

Canon Medical Products under investigation : None

Resolution: Not Applicable

Notes:

Continue to check this advisory for updated information.

Please email **CybersecurityRiskManagement@us.medical.canon** with any specific questions or issues.

Additional Notes:

As reported by Armis, https://www.armis.com/urgent11/, there are five more CVE's, shown below, that may lead to Denial of Service. These CVE's follow the same response as the CVE's noted earlier in this advisory.

- CVE-2019-12258: https://nvd.nist.gov/vuln/detail/CVE-2019-12258
- CVE-2019-12262: https://nvd.nist.gov/vuln/detail/CVE-2019-12262
- CVE-2019-12264: https://nvd.nist.gov/vuln/detail/CVE-2019-12264
- CVE-2019-12259: https://nvd.nist.gov/vuln/detail/CVE-2019-12259
- CVE-2019-12265: https://nvd.nist.gov/vuln/detail/CVE-2019-12265

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life