Wind River VxWorks - URGENT/11 Vulnerability

Publication Date: 2019-08-26

Last Update: 2019-08-26

CVSS v3.0:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 3.9

Description

on August 08, 2019, 11 cybersecurity vulnerabilities regarding Wind River VxWorks Operating system have been announced. This set of vulnerabilities is known as URGENT/11. These vulnerabilities are classified as critical and can enable Remote Code Execution.

Product Status

SuperSonic medical devices are not affected by the following CVE:

CVE-2019-12256	Stack overflow in the parsing of IPv4 packets' IP options
CVE-2019-12257	Heap overflow in DHCP Offer/ACK parsing inside ipdhcpc
CVE-2019-12255	TCP Urgent Pointer = 0 leads to integer underflow
CVE-2019-12260	TCP Urgent Pointer state confusion caused by malformed TCP AO option
CVE-2019-12261	TCP Urgent Pointer state confusion during connect() to a remote host
CVE-2019-12263	TCP Urgent Pointer state confusion due to race condition
CVE-2019-12258	DoS of TCP connection via malformed TCP options
CVE-2019-12259	DoS via NULL dereference in IGMP parsing
CVE-2019-12262	Handling of unsolicited Reverse ARP replies (Logical Flaw)
CVE-2019-12264	Logical flaw in IPv4 assignment by the ipdhcpc DHCP client
CVE-2019-12265	IGMP Information leak via IGMPv3 specific membership report

Additional Information:

For additional information on these vulnerabilities, please visit:

- US-CERT advisory ICSA-19-211-01; and
- Armis team's Urgent/11 web page.

For further information on product's security please visit our product security page: https://www.supersonicimagine.com/security