Security Advisory

2020-12-08-01 SecurityAdvisory.pdf

Metadaten

Published: 08.Dez. 2020
Version:1.0

Affected Products

Products	Affected Firmware Versions	Patched Firmware Version	Recommended Firmware Version
CPR50.10-E	<= 02.09.00	02.10.00	02.11.00
MAX50.10-xE	<= 02.09.00	02.10.00	02.11.00
MRU102-PoE	<= 01.04.00	01.05.00	02.01.00
MRU200-E*	<=03.01.00	End-of-Live	End-of-Live
MR102-PoE	<=02.04.00	02.05.00	02.11.00
LR1002-E	<=01.03.00	01.04.00	02.01.00
LR2500-B	<=01.07.00	01.08.00	02.06.00
ANT1800/700-A	<=01.07.00	01.08.00	02.06.00
ANT1690/600-A	<=01.07.00	01.08.00	02.06.00
ANT1700/740-A	<=01.07.00	01.08.00	02.06.00
ANT1700/740-SLA	<=01.07.00	01.08.00	02.06.00
ANT1300/680-A	<=01.03.00	01.04.00	02.01.00

* discontinued; delivered until 2016

Summary

FEIG is aware of multiple security vulnerabilities in the uIP stack - commonly referred to as "AMNESIA:33". A number of FEIG products use this stack and are therefore vulnerable to Denial of Service attacks via the network if operated with back level firmware. FEIG recommends to check the firmware level of affected products and conduct the actions detailed below, if applicable.

Vulnerability ID

CVE ID: CVE-2020-13988, CVE-2020-13987, CVE-2020-17438, CVE-2020-17440, CVE-2020-17439, CVE-2020-17437, CVE-2020-24334

Vulnerability Severity

CVE-ID	CVSS 3.0 score	CVSS 3.0 vector
CVE-2020-13988	7,5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2020-13987	8,2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H
CVE-2020-17438	7	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H
CVE-2020-17440	7,5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2020-17439	8,1	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L
CVE-2020-17437	8,2	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
CVE-2020-24335	7,5	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVE-2020-24334	8,2	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Vulnerability Details

The affected products and firmware versions use the Open-Source TCP/IP stack uIP. Vulnerabilities exist in the uIP TCP/IP stack included in the firmware versions listed above. An attacker who successfully exploits these vulnerabilities could allow attackers to hijack existing TCP sessions to perform Denial of Service (DoS) attacks.

CVE-2020-13988: An attacker who is in the position to send arbitrary TCP packets to an affected device can cause device firmware to run into an infinite loop. Due to watchdog supervision the device will reboot. If the attacker is in the position to send TCP packets with a sufficiently high frequency he can thus cause a Denial of Service.

CVE-2020-13987: An attacker who is in the position to send arbitrary TCP packets to an affected device can cause device firmware to reboot. If the attacker is in the position to do this with a sufficiently high frequency he can thus cause a Denial of Service.

CVE-2020-17438: FEIG readers are not vulnerable w.r.t. this CVE.

CVE-2020-17440: FEIG readers are not vulnerable w.r.t. this CVE.

CVE-2020-17439: FEIG readers are not vulnerable w.r.t. this CVE.

CVE-2020-17437: FEIG readers are not vulnerable w.r.t. this CVE.

CVE-2020-24334: FEIG readers are not vulnerable w.r.t. this CVE.

Recommended immediate actions

The issue is corrected in the firmware versions listed above. FEIG ELECTRONIC recommends that customers apply the update at the earliest convenience.
If firmware updates can not be applied we strongly recommend to protect your network such that attackers can not send TCP packets to affected devices.

Link Download Area: https://www.feig.de/en/login/

Acknowledgments

We thank Jos Wetzels, Stanislav Dashevskyi, Amine Amri, and Daniel dos Santos at Forescout Technologies for reporting this vulnerability following coordinated disclosure and BSI und CISA for coordinating.

Disclaimer