Security Advisory

Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33) in VARIOMOD XC $^{\text{ETH}}$

Document ID:	EMH-2021-001
Publication Date:	03.02.2021
Version:	1.0

SUMMARY

Recently security researchers discovered and disclosed 33 vulnerabilities in several open-source TCP/IP stacks (uIP, FNET, open-iscsi, picoTCP and Nut/Net) for embedded devices, also known as “AMNESIA:33” vulnerabilities. Our product Variomod XC Ethernet (VAXCET) is affected by 7 of these vulnerabilities (CVE-2020-13987, CVE-2020-13988, CVE-2020-17437, CVE-2020-17438, CVE-2020-17439, CVE-2020-17440 and CVE-2020-24334). EMH metering released a new firmware that eliminates all vulnerabilities and recommends specific countermeasures for vulnerable versions.

AFFECTED PRODUCTS AND SOLUTION

Affected products and Versions	Solution / Remediation
Variomod XC Ethernet (VAXCET), Version 1.13.6 and prior	Update to 1.13.7 or later version Firmware is available via Support

VULNERABILITY DETAILS

These vulnerabilities primarily cause memory corruption, allowing attackers to compromise devices, execute malicious code, perform denial-of-service attacks and get access to unauthorized data.

For more details regarding the AMNESIA:33 vulnerabilities in embedded TCP/IP stacks click the CVE links above or refer to:

- Forescout Publication “AMNESIA:33”
- CERT/CC Advisory VU#815128
- CISA Industrial Control Systems Advisory ICSA-20-343-01

WORKAROUNDS AND MITIGATIONS

EMH metering has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to the device to the internal or VPN network and to trusted IP addresses only.
- Do not use hostnames for the FTP, IPT or NTP server, only IP addresses.

ACKNOWLEDGMENTS

EMH metering thanks the following parties for their efforts:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordinated disclosure
- Jos Wetzels, Stanislav Dashevskyi, Amine Amri, and Daniel dos Santos from Forescout Technologies for researching and reporting these vulnerabilities.

CONTACT INFORMATION

For any questions related to this report, please contact EMH metering:

Tel.: +49 38851 326-0
Fax: +49 38851 326-1129
E-Mail: info@emh-metering.com
Web: www.emh-metering.com\

EMH metering continuously strives to improve its products and services.
If you have any suggestions or improvements to our products and services, please don’t hesitate to contact us.