Miele Product Security Incident Response Team - Advisory

Treck TCP/IP Vulnerabilities (Ripple20) affecting Ethernet Communication Module XKM3000 L MED

This advisory is subject to change

Issued:	08.07.2020
Issuer:	Miele PSIRT, psirt@miele.com
Advisory ID:	Miele-2020-002
Reference ID:	VDE-2020-024
Overall Criticality / CVSS:	10.0 (Critical)
Last Update:	08.07.2020
Classification:	Public

CVE Identifier

CVE-2020-11896, CVE-2020-11897, CVE-2020-11898, CVE-2020-11899, CVE-2020-11900, CVE-2020-11901, CVE-2020-11902, CVE-2020-11903, CVE-2020-11904, CVE-2020-11905, CVE-2020-11906, CVE-2020-11907, CVE-2020-11908, CVE-2020-11909, CVE-2020-11910, CVE-2020-11911, CVE-2020-11912, CVE-2020-11913, CVE-2020-11914

Severity

10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Affected Products

Tech Type	Materialnumber	Software Version
XKM3000 L MED	09902230 10440980	Modul Softwareversion <= 1.9.X

The above named communication module can be integrated into the following laboratory washers, thermal disinfectors and washer-disinfectors:

Tech Type
PG 8581, PG 8582, PG 8583, PG 8583 CD, PG 8591, PG 8582 CD, PG 8592, PG 8593, PG 8562

Miele Product Security Incident Response Team - Advisory

Vulnerability Type

CWE-130: Improper Handling of Length Parameter Inconsistency

Summary

For process data documentation purposes the laboratory washers, thermal disinfectors and washer-disinfectors can be integrated in a TCP/IP network by utilizing the affected communication module.

The communication module is separated from the devices internal control units. It contains a chipset of the company Digi International. The necessary TCP/IP stack within this chipset is based on a 3rd party library provided by the company Treck. External security researchers identified multiple security issues named Ripple20 within this library. The most critical issue allows an external attacker to execute arbitrary code on the chipset and therefore the named communication module.

Impact

The most critical security issue is described here. All other issues are listed in the CVE list above or within the sources provided below.

Vulnerability ID	CVE-2020-11896
Type	CWE-130: Improper Handling of Length Parameter Inconsistency
Vulnerability / Issues	Improper handling of length parameter within the IPv4/UDP component processing a package send by an unauthorized attacker. An attacker might execute arbitrary code on the communication module.
CVSS Score	10.0 (Critical)
CVSS v3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

The communication modules intended functionality (process documentation) cannot be guaranteed after a successful attack – authenticity availability and integrity of the data are at risk.

The security issue has no impact on the devices safety and cleaning and disinfection results of the laboratory washers, thermal disinfectors and washer-disinfectors.

Solution / Mitigation Measures

A security patch will be installed on the devices during regular maintenance and device requalification by the Miele customer service or authorized service partners.

Temporary Mitigation

The intended use of the devices and the networking functionalities do not require internet connection. Please operate the devices only in a secure local network to further reduce the risk.

Sources

- https://www.kb.cert.org/vuls/id/257161
- https://www.us-cert.gov/ics/advisories/icsa-20-168-01