Miele Product Security Incident Response Team - Meldung

Treck TCP/IP Sicherheitslücken (Ripple20) betreffen Ethernet Kommunikationsmodul XKM3000 L MED

Diese Meldung ist nur in ihrer aktuellsten Fassung gültig.

Veröffentlichungsdatum:	08.07.2020
Herausgeber:	Miele PSIRT, psirt@miele.com
Meldungs ID:	Miele-2020-002
Referenz ID:	VDE-2020-024
Kritikalität / CVSS:	10.0 (Kritisch)
Letzte Aktualisierung:	08.07.2020
Klassifizierung	Öffentlich

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

Schweregrad

10.0 (Kritisch)

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

Betroffene Produkte

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

Das Kommunikationsmodul kann in folgenden Laborspülern, Thermodesinfektoren und Reinigungs-/Desinfektionsgeräten eingesetzt werden:

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 - Meldung

Typ der Sicherheitslücke

CWE-130: Improper Handling of Length Parameter Inconsistency

Zusammenfassung

Zum Zwecke der Prozessdatendokumentation können die genannten Laborspüler, Thermodesinfektoren und Reinigungs-/Desinfektionsgeräte mit Hilfe des genannten Kommunikationsmoduls in ein TCP/IP Netzwerk integriert werden.

Das Kommunikationsmodul ist von der eigentlichen Gerätesteuerung getrennt und setzt einen Chipsatz der Firma Digi International ein. Der für die Vernetzung notwendige TCP/IP Stack wird bei diesem Chipsatz mit Hilfe einer 3rd Party Bibliothek der Firma Treck realisiert. Externe Sicherheitsforscher haben in dieser Bibliothek mehrere Sicherheitslücken mit dem Namen Ripple20 identifiziert. Dabei erlaubt die kritischste Lücke einem externen Angreifer möglicherweise beliebigen Code auf dem Chip und damit auch auf dem Kommunikationsmodul auszuführen.

Auswirkung

Hier wird nur die Schwachstelle mit der höchsten Kritikalität genannt. Alle weiteren Schwachstellen sind in der CVE Liste oben oder in den unten gelisteten Quellen aufgeführt.

Vulnerability ID	CVE-2020-11896
Type	CWE-130: Improper Handling of Length Parameter Inconsistency
Vulnerability / Issues	Unsachgemäße Behandlung der Längenparameter in der IPv4/UDP-Komponente bei der Verarbeitung eines empfangenen Pakets. Ein Angreifer kann möglichweise beliebigen Code auf dem Modul ausführen.
CVSS Score	10.0 (Kritisch)
CVSS v3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Die bestimmungsgemäße Funktion des Moduls (Ermöglichung der Prozessdatendokumentation) kann nach einem erfolgreichen Angriff nicht mehr garantiert werden – Authentizität, Verfügbarkeit und Integrität der Daten sind gefährdet.

Die Sicherheitslücke hat keine Auswirkung auf die Gerätesicherheit und Reinigungs- und Desinfektionsergebnisse der genannten Laborspüler, Thermodesinfektoren und Reinigungs-/Desinfektionsgeräte.

Lösung / Maßnahmen zur Schließung der Sicherheitslücken

Ein Sicherheitsupdate wird im Rahmen der regelmäßigen Wartung und Requalifizierung durch den Miele Kundendienst oder autorisierte Servicepartner auf dem Modul installiert.

Kurzfristige Maßnahmen

Die vorgesehene Nutzung der Laborspüler, Thermodesinfektoren und Reinigungs-/Desinfektionsgeräte und der dazugehörigen Vernetzungsfunktionen setzen keine Internetverbindung voraus. Bitte betreiben Sie das Produkt ausschließlich in einem gesicherten lokalen Netzwerk.

Quellen

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