Miele Security Meldung

# Sicherheitslücken in XGW 3000 ZigBee Gateway

Das XGW 3000 ZigBee Gateway in den Softwareversionen <= 2.3.4 (1.4.6) ist von mehreren Sicherheitslücken betroffen.

**Diese Meldung ist nur in ihrer aktuellsten Fassung gültig.**

| | |
|---|---|
| **Veröffentlichungsdatum** | 17.05.2019 |
| **Herausgeber** | Miele PSIRT, CERT@VDE |
| **Meldungs ID** | Miele-2019-001 |
| **Referenz ID** | VDE-2019-010, CVE-2019-20480, CVE-2019-20481 |
| **Kritikalität / CVSS** | 4.4 (Mittel) |
| **Letztes Update** | 25.02.2020 |

## CVE ID

CVE-2019-20480, CVE-2019-20481

## Schweregrad

4.4 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C)

## Betroffene Produkte

| Product | Software Version |
|---|---|
| XGW 3000 ZigBee Gateway | <= 2.3.4 (1.4.6) |

## Typ der Sicherheitslücke

Unsachgemäße Autorisierung (CWE-285)

Cross-Site Request Forgery (CWE-352)

## Zusammenfassung

Das Miele XGW 3000 ist ein ZigBee-TCP/IP Gateway. Miele Haushaltsgeräte mit ZigBee Konnektivität (Miele@home) können über das Gateway mit einem lokalen TCP/IP basierten Netzwerk verbunden werden. Anschließend können die Statusinformationen der verbundenen Geräte über die Weboberfläche das Gateways, Miele Geräte mit SuperVision Unterstützung, Mobilen Endgeräten (mittels Miele@mobile App) oder ausgewählten Hausautomatisierungssystemen angezeigt werden.

Ein externer Sicherheitsforscher hat Miele über die Existenz zweier zusammenhängender und ausnutzbarer Sicherheitslücken im XGW 3000 Gateway informiert. Eine gleichzeitige Ausnutzung beider Lücken erlaubt es, die passwortgeschützte Anmeldefunktion des Gateways zu umgehen.

Das Miele PSIRT (Product Security Incident Response Team) konnte die gemeldeten Lücken reproduzieren und bestätigen.

# Miele Security Meldung

## Auswirkung

| | |
|---|---|
| **Vulnerability ID** | PSIRT-2019-001-VI_01 |
| **Type** | CWE-352: Cross-Site Request Forgery (CSRF) |
| **Vulnerability / Issues** | Eine bösartige Website, die von einem authentifizierten Admin-Benutzer besucht wird, kann bestimmte Änderungen im "Admin-Panel" vornehmen. |
| **CVSS Score** | Medium (4.4) |
| **CVSS v3 Vector** | AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C |

| | |
|---|---|
| **Vulnerability ID** | PSIRT-2019-001-VI_02 |
| **Type** | CWE-285: Unsachgemäße Autorisierung |
| **Vulnerability / Issues** | Umgehen der Authentifizierungsfunktion. In Kombination mit der Sicherheitslücke PSIRT-2019-001-VI_01 (CSRF), kann das Passwort des Administrators geändert werden ohne das aktuelle zu prüfen. |
| **CVSS Score** | Medium (4.4) |
| **CVSS v3 Vector** | AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:L/E:P/RL:X/RC:C |

## Lösung / Maßnahmen zur Schließung der Sicherheitslücken

Installieren der Gerätesoftware in der Version **2.4.0 (oder größer)** über die automatische Updatefunktion des XGW 3000 ZigBee Gateway.

Hierzu an der lokalen Miele@home Admin Website des XGW 3000 Gateways anmelden. Anschließend auf → *Einstellungen* → *Update* → *Neu Software (oder neue Firmware) suchen* klicken. Die aktuellste Version wird dann zur Installation vorgeschlagen. Bitte nach der Installation prüfen, ob die Gateway Software mindestens in der Version 2.4.0 oder größer angezeigt wird. Sollte dies nicht er fall sein, ist der Updateprozess erneut durchzuführen.

## Quellen

https://psirt.miele.com

https://cert.vde.com/de-de/advisories

## Danksagung

Wir möchten uns bei **Maxim Rupp / rupp.it** bedanken, der die genannten Lücken identifiziert und vertrauensvoll an das Miele PSIRT gemeldet hat.