Miele Security Advisory

Multiple Vulnerabilities in XGW 3000 ZigBee Gateway

XGW 3000 is prone to vulnerabilities in version <= 2.3.4 (1.4.6)

This advisory is subject to change

Issued:	17.05.2019
Issuer:	Miele PSIRT, CERT@VDE
Advisory ID	Miele-2019-001
Reference ID:	VDE-2019-010, CVE-2019-20480, CVE-2019-20481
Overall Criticality / CVSS:	4.4 (Medium)
Last Update:	25.02.2020

CVE Identifier

CVE-2019-20480, CVE-2019-20481

Severity

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)

Affected Products

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

Vulnerability Type

Improper Authorization (CWE-285)

Cross-Site Request Forgery (CWE-352)

Summary

Miele XGW 3000 is a ZigBee-TCP/IP gateway. The gateway connects Miele ZigBee-Appliances (called Miele@home) with local customer TCP/IP-Network and allows visualizing the appliance state on the web interface of the gateway, Miele SuperVision capable appliance, smartphone/tablet app or home automatization device.

An external security researcher reported two vulnerabilities in XGW 3000 gateway and provided a Proof-of-Concept. The combined exploitation of both vulnerabilities allow the circumvention of the authentication mechanisms of the XGW3000.

The Miele PSIRT managed to reproduce the findings and successfully exploited the gateway. Therefore, the existence of all vulnerabilities has been confirmed.

Miele Security Advisory

Impact

Vulnerability ID	PSIRT-2019-001-VI_01
Type	CWE-352: Cross-Site Request Forgery (CSRF)
Vulnerability / Issues	A malicious website visited by an authenticated admin user is allowed to issue certain changes in the "admin panel".
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: Improper Authorization
Vulnerability / Issues	Bypass for "Password Change Function". In combination of vulnerability PSIRT-2019-001-VI_01 (CSRF), the administrator password can be changed without checking the old one.
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

Solution

Install software version **2.4.0** via the automatic update function of the XGW 3000 ZigBee Gateway.

To do so, log into the local Miele@home Gateway Info Admin Panel. Afterwards, click on *Settings* → Click on *Update* → Click on *Check for New Software*. The latest version of the Gateway software will be suggested for installation. After the installation has been completed, verify if the installed version is 2.4.0 or larger. If this is not the case, the update process has to be started a second time.

Published at

https://psirt.miele.com

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

Reported by

We would like to thank **Maxim Rupp / rupp.it** for reporting this issue to Miele PSIRT.