Miele Product Security Incident Response Team - Advisory

Vulnerability in ease2pay cloud service used by appWash

This message is only valid in its most current version.

Release Date:	21.11.2022
Publisher:	Miele PSIRT
Internal message ID:	PSI22101
Reference ID:	CVE-2022-3589
Criticality / CVSS v3.1:	8.1 (High)
Last updated:	21.11.2022
Classification	Public

CVE ID

CVE-2022-3589

Severity

Base Score: 8.1 (CVSS:3.1:AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

Affected products

Product	**Software version**
ease2pay cloud service used by appWash	before 05.10.2022

Vulnerability type

CWE-639: Authorization Bypass Through User-Controlled Key

Summary

Up until October 5th, 2022 the ease2pay API used by Miele's "AppWash" MobileApp was vulnerable to an authorization bypass.
A low privileged, remote attacker would have been able to gain read and partial write access to other users data by modifying a small part of a HTTP request sent to the API. Reading or changing the password of another user was not possible, thus no impact to Availability.

Impact

The evaluation of the log files by ease2pay did not show any sign of actual exploitation of the vulnerability, extraction of data or misuse.

Solution / measures to close the security gaps

The ease2pay cloud service used by appWash was fixed on 05.10.2022. The tokens used for session authentication were changed to a secure state of the art solution. All affected tokens have been invalidated and new tokens were issued. Therefore, no actions have to be taken by the users.

Sources

https://psirt.miele.com

https://cert.vde.com/en/advisories/

Acknowledgement / Reported by

CERT@VDE coordinated with Miele.

We would like to thank Bishoy Roufael for reporting this issue to Miele PSIRT.