Miele Product Security Incident Response Team - Advisory

Sicherheitslücke in Ease2pay (verwendet von appWash)

Diese Meldung ist nur in ihrer aktuellen Fassung gültig.

Veröffentlichungsdatum:	21.11.2022
Herausgeber:	Miele PSIRT
Interne Meldungs ID:	PSI22101
Referenz ID:	CVE-2022-3589
Kritikalität / CVSS v3.1:	8.1 (High)
Letzte Aktualisierung:	21.11.2022
Klassifizierung	Öffentlich

CVE ID

CVE-2022-3589

Schweregrad

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

Betroffene Produkte

Produkt	Software version
ease2pay Cloud Service (verwendet von appWash)	vor dem 05.10.2022

Typ der Sicherheitslücke

CWE-639: Authorization Bypass Through User-Controlled Key

Zusammenfassung

Bis zum 5. Oktober 2022 war die ease2pay API, die von der Miele MobileApp AppWash verwendet wird, anfällig für eine Sicherheitslücke (Authorization Bypass).
Ein Angreifer mit geringen Privilegien hätte über das Internet Lese- und teilweise Schreibzugriff auf die Daten anderer Benutzer erlangen können, indem er einen kleinen Teil einer HTTP Anfrage, die an die API gesendet wird, modifiziert.
Das Lesen oder Ändern des Passworts eines anderen Benutzers war nicht möglich, so dass die Verfügbarkeit nicht beeinträchtigt wurde.

Auswirkung

Die Auswertung der Logdateien durch ease2pay ergab keine Anzeichen für eine tatsächliche Ausnutzung der Schwachstelle, eine Extraktion von Daten oder einen Missbrauch.

Lösung / Maßnahmen zur Schließung der Sicherheitslücken

Der von appWash verwendete Cloud-Dienst ease2pay wurde am 05.10.2022 angepasst. Die für die Sitzungsauthentifizierung verwendeten Token wurden auf eine sichere, dem neuesten Stand der Technik entsprechende Lösung umgestellt. Alle betroffenen Token wurden für ungültig erklärt und neue Token wurden ausgegeben. Daher müssen die Benutzer keine Maßnahmen ergreifen.

Quellen

https://psirt.miele.com

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

Danksagung

CERT@VDE koordiniert mit Miele.

Wir bedanken uns bei Bishoy Roufael für die Identifikation und schnelle Meldung der Sicherheitslücke.