

# Sicherheitslücke im Miele Benchmark Programming Tool

Diese Meldung ist nur in ihrer aktuellen Fassung gültig.

Veröffentlichungsdatum:	27.04.2022
Herausgeber:	Miele PSIRT
Interne Meldungs ID:	PSI22032
Referenz ID:	CVE-2022-22521
Kritikalität / CVSS v3.1:	7.3 (High)
Letzte Aktualisierung:	12.05.2022
Klassifizierung	Öffentlich

## CVE ID

CVE-2022-22521

## Schweregrad

[3.1 \(CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H\) \(7.3 High\)](#)

## Betroffene Produkte

Produkt	Software version
Benchmark Programming Tool	1.2.71 und älter

## Typ der Sicherheitslücke

Improper Privilege Management (CWE-269)

## Zusammenfassung

Das Miele Benchmark Programming Tool ist eine Desktop-Anwendung, die es dem Anwender unter anderem ermöglicht, Waschmaschinen- und Wäschetrocknerprogramme sowie Maschineneinstellungen an seinen Miele Professional-Geräten komfortabel zu bearbeiten.

Es wurde festgestellt, dass bei der Installation des Miele Benchmark Programming Tool auf einem Microsoft Windows Betriebssystem standardmäßig ein Installationsordner gewählt wird, der für alle Benutzer beschreibbar ist (C:\MIELE\_SERVICE). Nach der Installation des Tools, ist es daher möglich, dass auch Benutzer ohne administrative Berechtigungen ausführbare Dateien in diesem Pfad austauschen oder löschen können.

## Miele Product Security Incident Response Team - Advisory

### Auswirkung

<b>Vulnerability ID</b>	PSI22032
<b>Type</b>	<a href="#">CWE-269: Improper Privilege Management</a>
<b>Vulnerability / Issues</b>	Durch Angreifer manipulierte ausführbare Dateien werden unwissentlich durch Benutzer mit administrativen Berechtigungen ausgeführt. Ein Angreifer kann dadurch bspw. selbst höhere Berechtigungen erhalten. Der Angreifer muss bereits Zugriff auf das entsprechende lokale System haben, um die Dateien austauschen zu können.
<b>CVSS Score v3.1</b>	7.3 High
<b>CVSS v3.1 Vector</b>	<a href="#">3.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)</a>

### Lösung / Maßnahmen zur Schließung der Sicherheitslücken

#### Update des Benchmarking Programming Tool

Eine neue Version (1.2.72) des Benchmark Programming Tools, welche die benannte Lücke schließt, steht auf der Miele Website zum Download bereit:

<https://www.miele.de/p/miele-benchmark-programming-tool-2296.htm>

#### Anpassen der Ordner Berechtigungen

Als weitere risikominimierende Maßnahme, können die Schreibberechtigungen des Installationsordners C:\Miele\_Service\Miele Benchmark Programming Tool so angepasst werden, dass ein Austausch der Dateien nur noch mit administrativen Berechtigungen möglich ist. Dies ist auch ohne Neuinstallation oder Update des Tools möglich. Das Vorgehen zum Anpassen der Berechtigungen ist abhängig von der jeweils genutzten Microsoft Windows Betriebssystem Umgebung und benötigt in den meisten Fällen administrative Rechte.

### Quellen

<https://sec-consult.com/vulnerability-lab/>

### Danksagung

Wir bedanken uns bei SEC Consult Vulnerability Lab für die Identifikation und schnellen Meldung der Sicherheitslücke.