

Security vulnerability affecting Miele Benchmark Programming Tool

This message is only valid in its most current version.

Release Date:	27.04.2022
Publisher:	Miele PSIRT
Internal message ID:	PSI22032
Reference ID:	CVE-2022-22521
Criticality / CVSS v3.1:	7.3 (High)
Last updated:	12.05.2022
Classification	Public

CVE ID

CVE-2022-22521

Severity

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

Affected products

Product	Software version
Benchmark Programming Tool	1.2.71 and older

Vulnerability type

Improper Privilege Management (CWE-269)

Summary

The Miele Benchmark Programming Tool is a desktop application that allows users, among other things, to edit washing machine and tumble dryer programs and machine settings on their Miele Professional appliances.

It was discovered, that when installing the Miele Benchmark Programming Tool on a Microsoft Windows operating system, an installation folder is selected by default that is writable for all users (C:\MIELE_SERVICE). After the installation of the tool, users without administrative privileges are able to exchange or delete executable files in this path.

Miele Product Security Incident Response Team - Advisory

Impact

Vulnerability ID	PSI22032
Type	CWE-269: Improper Privilege Management
Vulnerability / Issues	Executable files manipulated by attackers are unknowingly executed by users with administrative privileges. An attacker could thereby obtain higher permissions. The attacker must already have access to the corresponding local system to be able to exchange the files.
CVSS Score v3.1	7.3 High
CVSS v3.1 Vector	3.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)

Solution / measures to close the security gaps

Update of the Benchmarking Programming Tool

A new version (1.2.72) of the Benchmark Programming Tool, which closes the named vulnerability, is available for download on the Miele website:

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

Customize the folder permissions

As a further risk-minimizing measure, the write permissions of the installation folder C:\Miele_Service\Miele Benchmark Programming Tool can be adjusted so that an exchange of files is only possible with administrative permissions. This is also possible without reinstalling or updating the tool. The procedure for adjusting the permissions depends on the Microsoft Windows operating system environment used and in most cases requires administrative rights.

Sources

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

Acknowledgement / Reported by

We would like to thank SEC Consult Vulnerability Lab for identifying and quickly reporting the vulnerability to Miele PSIRT.