

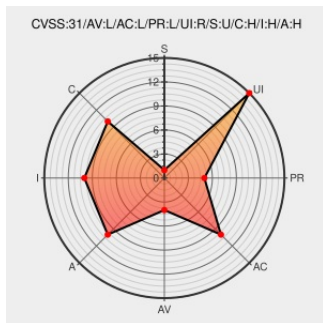


CVE-2022-22521

Published on: Not Yet Published

Last Modified on: 08/09/2023 11:15:00 AM UTC

CVE-2022-22521

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Benchmark Programming Tool](#) from [Miele](#) contain the following vulnerability:

In Miele Benchmark Programming Tool with versions Prior to 1.2.71, executable files manipulated by attackers are unknowingly executed with users privileges. An attacker with low privileges may trick a user with administrative privileges to execute these binaries as admin.

CVE-2022-22521 has been assigned by [cert](#) info@cert.vde.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cert](#) **Miele - Benchmark Programming Tool** version = 1.2.71

Vulnerability Patch/Work Around

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.

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
VDE-2022-015 CERT@VDE	cert.vde.com text/html	 CONFIRM cert.vde.com/en/advisories/VDE-2022-015/
Miele Benchmark Programming Tool	www.miele.de text/html	 MISC www.miele.de/p/miele-benchmark-programming-tool-2296.htm
Full Disclosure: SEC Consult SA-20220427-0 :: Privilege Escalation in Miele Benchmark Programming Tool	seclists.org text/html	 FULLDISC 20220427 SEC Consult SA-20220427-0 :: Privilege Escalation in Miele Benchmark Programming Tool
Miele Benchmark Programming Tool 1.1.49 / 1.2.71 Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/166881/Miele-Benchmark-Programming-Tool-1.1.49-1.2.71-Privilege-Escalation.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miele	Benchmark Programming Tool	All	All	All	All
cpe:2.3:a:miele:benchmark_programming_tool:*:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-22521 : In Miele Benchmark Programming Tool with versions Prior to 1.2.71, executable files manipulated by... twitter.com/i/web/status/1...	2022-04-27 15:18:55
 /r/netcve	CVE-2022-22521	2022-04-27 16:39:08

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

