SEC Consult SA-20220427-0 :: Privilege Escalation in Miele Benchmark Programming Tool

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists org>
Date: Wed, 27 Apr 2022 05:34:52 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20220427-0 >
=======================================================================
               title: Privilege Escalation
             product: Miele Benchmark Programming Tool
  vulnerable version: at least 1.1.49 and 1.2.71
       fixed version: 1.2.72
          CVE number: CVE-2022-22521
              impact: Medium
            homepage: https://www.miele.com/
               found: 2022-01-24
                  by: J. Kruchem (Office Vienna)
                      W. Schober (Office Vienna)
                      SEC Consult Vulnerability Lab

                      An integrated part of SEC Consult, an Atos company
                      Europe | Asia | North America

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"There are many good reasons for choosing Miele. Since the company's founding in
1899, Miele has remained true to its "Immer Besser" brand promise. This means
that we will do all that we can to be "Immer Besser" (forever better) than our
competitors and "Immer Besser" (forever better) than we already are. For our
customers, this means the peace of mind of knowing that choosing Miele is a
good decision - and probably the decision of a lifetime."

Source: https://www.mieleusa.com/c/about-us-9.htm


Business recommendation:
------------------------
The vendor provides a patched version which should be installed immediately.

An in-depth security analysis performed by security professionals is highly advised,
as the software may be affected from further security issues.
```

Vulnerability overview/description:
----
1) Privilege Escalation (CVE-2022-22521)
The path where the Miele Benchmark Programming Tool is installed is writable
for any user on the Windows operation system. This allows replacing the Uninstall
binary and thus an attacker gaining local admin privileges if uninstalled.

Proof of concept:
----
1) Privilege Escalation (CVE-2022-22521)
The Uninstall string can be found in the following registry entry:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall
\{<UUID of Miele Benchmark
Programming>}

The UninstallString field has the following value:

UninstallString
"C:\MIELE_SERVICE\Miele Benchmark Programming Tool\Uninstall Miele Benchmark Programming
Tool.exe" /allusers

For exploitation, replace the "Uninstall Miele Benchmark Programming Tool.exe"
with a malicious binary and uninstall via Software Center or call the admin
and let them uninstall the Miele Benchmark Programming Tool.

Vulnerable / tested versions:

The following versions have been tested, which were the latest versions available
during the time of the test:

* 1.1.49
* 1.2.71

Other (lower) software versions may be affected as well.

Vendor contact timeline:

2022-03-21: Contacting vendor through psirt () miele com
2022-03-22: Vendor answered that they will check the provided information
2022-04-07: Vendor confirmed the vulnerability and answered with aim to fix it asap
2022-04-11: Vendor sent their advisory (including CVE) and fixed version
2022-04-27: Coordinated release of advisory.

Solution:

The vendor provides a patched version v1.2.72 which can be downloaded here:

https://www.miele.com/en/com/downloads-6770.htm

Workaround:

Adapt permissions of the C:\MIELE_SERVICE directory according to the least privilege
principle.

Advisory URL:
----

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

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~

Mail: security-research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF J. Kruchem / @2022

By Date By Thread

Current thread:

SEC Consult SA-20220427-0 :: Privilege Escalation in Miele Benchmark Programming Tool *SEC Consult Vulnerability Lab, Research via Fulldisclosure (Apr 27)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License
~~~~~~