Miele Benchmark Programming Tool 1.1.49 / 1.2.71 Privilege Escalation

Authored by W. Schober, Johannes Kruchem | Site sec-consult.com

Posted Apr 27, 2022

Miele Benchmark Programming Tool versions 1.1.49 and 1.2.71 suffer from a privilege escalation vulnerability.

tags | exploit
advisories | CVE-2022-22521
SHA-256 | d9c54518c9774d14210fa309ae32ce7bf54eac2d1ed82cd249dec9506f8662c7 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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:
```


File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
* 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
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed