README.md

Multiple vulnerabilities in Gurux GXDLMS Director – remote code execution

Gurux GXDLMS Director is an open-source Windows program for interacting with energy meters through the use of DLMS/COSEM protocol.

The software has a remote update functionality for add-in DLLs as well as for files containing OBIS codes (device-specific definitions needed to interact with the smart meters).

CVEID	Name of the affected product(s) and version(s)	Problem type
CVE-2020-8809	Gurux GXDLMS Director (all versions prior to 8.5.1905.1301)	CWE-494: Download of Code Without Integrity Check
CVE-2020-8810	Gurux GXDLMS Director (all versions)	CWE-23: Relative Path Traversal

Summary

All version of Gurux GXDLMS Director prior to 8.5.1905.1301 contain an update mechanism for add-ins and OBIS codes which works over an unencrypted HTTP connection. Additionally, all versions contain a path traversal bug which happens when downloading OBIS codes. Those vulnerabilities can be used by the attacker to achieve code execution.

Description

A man-in-the-middle attacker (e.g. a malicious Wi-Fi network operator) can prompt the user to download updates by modifying the contents of `gurux.fi/obis/files.xml` and `gurux.fi/updates/updates.xml` . Then, the attacker can modify the contents of downloaded files. In the case of add-ins (if the user is using those), this will lead to code execution. In case of OBIS codes (which the user is always using as they are needed to communicate with the energy meters), the attacker can achieve code execution by exploiting a path traversal vulnerability.

When downloading OBIS codes, the program does not verify that the downloaded files are actual OBIS codes and doesn’t check for path traversal. This allows the attacker to send executable files and place them in an autorun directory (run after reboot), or to place DLLs inside the existing GXDLMS Director installation (run on next execution of GXDLMS Director). This can be used to achieve code execution even if the user doesn’t have any add-ins installed.

Reproduction

1. Start an HTTP server.
2. Inside its root directory, create a directory called `obis` .
3. Create a file `obis/files.xml` with the following contents:

```
<files>
  <file modified=”28-09-2099” name=”Iskraemeco”>../../../../../../../../../../Users/Public/Documents/test.txt</file>
</files>
```

4. Create a directory `Users/Public/Documents` .
5. Create a file `Users/Public/Documents/test.txt` .
6. On a Windows machine, edit the file `C:\Windows\system32\drivers\etc\hosts` and add the following line to it: `127.0.0.1 gurux.fi` (if your HTTP server is not the same as your Windows machine, replace `127.0.0.1` with the server’s IP).
7. Start Gurux GXDLMS Director. When prompted to download an update, accept.
8. Verify that `C:\Users\Public\Documents\` now contains file `test.txt` .

Remedy

Update Gurux GXDLMS Director to the newest version.

No packages published