Talos Vulnerability Report

TALOS-2020-1167

Sytech XL reporter installation privilege escalation vulnerability

FEBRUARY 19, 2021

CVE NUMBER

CVE-2020-13549

Summary

An exploitable local privilege elevation vulnerability exists in the file system permissions of Sytech XL Reporter v14.0.1 install directory. Depending on the vector chosen, an attacker can overwrite service executables and execute arbitrary code with privileges of user set to run the service or replace other files within the installation folder, which would allow for local privilege escalation.

Tested Versions

Sytech XL Reporter v14.0.1

Product URLs

https://www.sytech.com/product-xlreporter-overview.asp

CVSSv3 Score

8.8 - CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CWE

CWE-276 - Incorrect Default Permissions

Details

XL Reporter is an industrial visualization and reporting software parsing data from PLC, HDA, OPC and historian systems.

By default, XL Reporter v14 is installed in “C:\XLReporter” directory and it allows “Authenticated Users” as well as “Everyone” group to have “Full/Change” privilege over “XLReporter Runtime” service binary file in the directory which are executed with NT SYSTEM authority. This allows users in both groups to read, write or modify arbitrary files in the install directory resulting in privilege escalation when service is restarted.

```
C:\XLReporter\bin\XLRiRuntime.exe
                              Everyone:(ID)F
                              BUILTIN\Administrators:(ID)F
                              NT AUTHORITY\SYSTEM:(ID)F
                              BUILTIN\Users:(ID)R
                              NT AUTHORITY\Authenticated Users:(ID)C
```

Timeline

2020-10-20 - Vendor Disclosure

2021-02-18 - Vendor Patched
2021-02-19 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.