Talos Vulnerability Report

TALOS-2021-1399

Advantech SQ Manager Server 1.0.6 privilege escalation vulnerability

JANUARY 18, 2022

CVE NUMBER

CVE-2021-40388

Summary

A privilege escalation vulnerability exists in Advantech SQ Manager Server 1.0.6. A specially-crafted file can be replaced in the system to escalate privileges to NT SYSTEM authority. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Advantech SQ Manager Server 1.0.6

Product URLs

https://www.advantech.com/support/details/utility?id=1-1YVUBC7

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

SQ Manager Server is a remote monitoring dashboard for manging SQRAM and SSD devices in IoT enviroments.

By default, Advantech SQ Manager Server is installed in the “c:\Program Files\Advantech" directory, which allows the “Everyone” group to have “Full” privilege over various service binary files in the directory, including library and executabes files loaded by the PostgreSQL service. The service execute these binaries with a “NT AUTHORITY\NETWORK SERVICE” privilege, leading to privilge escalation from ‘Everyone’ to ‘NETWORK SERVICE’ user when the file is replaced and service is restarted. As the services are assigned `SeImpersonatePrivilege` it is then possible to take advantage of that permission to achieve reliable execution with NT SYSTEM privilege due to impersonation of the token.

```
C:\Program Files\Advantech\SQ Manager Server\database\PostgreSQL\pgsql\bin\psql.exe Everyone:F

NT AUTHORITY\SYSTEM:F

C:\Program Files\Advantech\SQ Manager Server\database\PostgreSQL\pgsql\bin\postgres.exe Everyone:F

NT AUTHORITY\SYSTEM:F

C:\Program Files\Advantech\SQ Manager Server\database\PostgreSQL\pgsql\bin\pg_ctl.exe Everyone:F

NT AUTHORITY\SYSTEM:F
```

In addition, various DLL files can be used to perform similar exploitation of the system from the same installation folder:

```
libpq.dll
libeay32.dll
libiconv-2.dll
libintl-8.dll
ssleay32.dll
```

Timeline

2021-10-25 - Vendor Disclosure
2022-01-16 - Vendor Patched
2022-01-18 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1387

NEXT REPORT

TALOS-2021-1400