Talos Vulnerability Report

TALOS-2021-1409

Advantech WISE-PaaS/OTA 3.0.9 Server installation privilege escalation vulnerability

JANUARY 18, 2022

CVE NUMBER

CVE-2021-40397

Summary

A privilege escalation vulnerability exists in the installation of f Advantech WISE-PaaS/OTA Server 3.0.9. 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 WISE-PaaS/OTA Server 3.0.9

Product URLs

https://www.advantech.com/support/details/installation?id=1-1I77MDX

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

WISE-PaaS/OTA Server provides capability for Over The Air (OTA) updates to external IoT devices.

By default, WISE-PaaS/OTA Server is installed in the “c:\Program Files (x86)\Advantech\OTA 3.0 Server" 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 executes these binaries with a “NT AUTHORITY\NETWORK SERVICE” privilege, leading to an escalation from any user to ‘NETWORK SERVICE’ when the file is replaced and service is restarted. As the service is also 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 (x86)\Advantech\OTA 3.0 Server\Database\pgsql\bin\psql.exe
Everyone:F
NT AUTHORITY\SYSTEM:F

c:\Program Files (x86)\Advantech\OTA 3.0 Server\Database\pgsql\bin\pg_ctl.exe
Everyone:F
NT AUTHORITY\SYSTEM:F

c:\Program Files (x86)\Advantech\OTA 3.0 Server\Database\pgsql\bin\postgres.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

2021-11-02 - Vendor Disclosure
2022-01-16 - Vendor Patched
2022-01-18 - Public Release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.
