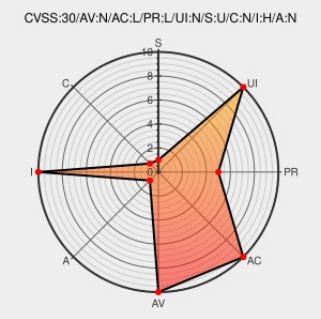
CVE-2018-15705

Published on: 10/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15705

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Webaccess from Advantech contain the following vulnerability:

WADashboard API in Advantech WebAccess 8.3.1 and 8.3.2 allows remote authenticated attackers to write or overwrite any file on the filesystem due to a directory traversal vulnerability in the writeFile API. An attacker can use this vulnerability to remotely execute arbitrary code.

CVE-2018-15705 has been assigned by vulnreport@tenable.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Advantech** - **Advantech WebAccess** version **8.3.1 and 8.3.2**

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 8.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Advantech WebAccess SCADA 8.3.2 - Remote Code Execution - ASP	Exploit	EXPLOIT-DB 45774

webapps Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	
[R1] Multiple Advantech WebAccess Vulnerabilities - Research Advisory | Tenable®	Exploit Third Party Advisory www.tenable.com text/html	MISC www.tenable.com/security/research/tra-2018-35

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Webaccess	8.3.1	All	All	All
Application	Advantech	Webaccess	8.3.2	All	All	All
Application	Advantech	Webaccess	8.3.1	All	All	All
Application	Advantech	Webaccess	8.3.2	All	All	All

cpe:2.3:a:advantech:webaccess:8.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:webaccess:8.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:webaccess:8.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:advantech:webaccess:8.3.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→