



CVE-2014-9202

Published on: 09/27/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

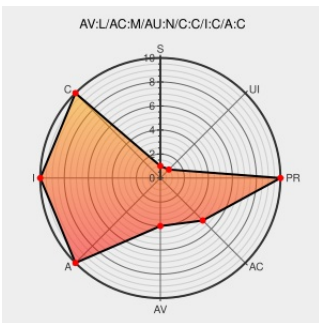
CVE-2014-9202

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Webaccess](#) from [Advantech](#) contain the following vulnerability:

Multiple stack-based buffer overflows in an unspecified DLL file in Advantech WebAccess before 8.0_20150816 allow remote attackers to execute arbitrary code via a crafted file that triggers long string arguments to functions.

CVE-2014-9202 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Advantech WebAccess Stack-Based Buffer Overflow Vulnerability
| ICS-CERT

Third Party Advisory

US Government Resource

ics-cert.us-cert.gov

text/html

MISC ics-cert.us-
cert.gov/advisories/ICSA-15-258-04

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)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Webaccess	8.0	All	All	All
Application	Advantech	Webaccess	8.0	All	All	All
cpe:2.3:a:advantech:webaccess:8.0:*:*:*:*:*:						
cpe:2.3:a:advantech:webaccess:8.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →