



CVE-2018-14816

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-14816
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-23 20:29:00 UTC
Updated	2023-11-07 02:53:00 UTC
Description	Advantech WebAccess 8.3.1 and earlier has several stack-based buffer overflow vulnerabilities that have been identified, w

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
Advantech WebAccess Bugs Let Remote Users Execute Arbitrary Code and Let Local Users Gain Elevated Privileges - SecurityTracker	SE
Advantech ICSA-18-296-01 WebAccess Multiple Security Vulnerabilities	BID
Page Not Found CISA	
404 - File Not Found CISA	MS
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

590844 Advantech WebAccess Multiple Vulnerabilities (ICSA-18-296-01)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)