



CVE-2018-18999

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-18999
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-19 18:29:00 UTC
Updated	2020-09-18 16:53:00 UTC
Description	WebAccess/SCADA, WebAccess/SCADA Version 8.3.2 installed on Windows 2008 R2 SP1. Lack of proper validation of us

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Advantech	Webaccess/scada	8.3.2	All	All	All
Application	Advantech	Webaccess/scada	8.3.2	All	All	All
Application	Advantech	Webaccess/scada	8.3.2	All	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All

References

Reference	Source	Link	Tags
Malformed Request	BID	www.securityfocus.com	Third Party Advi
Advantech WebAccess/SCADA CISA	MISC	ics-cert.us-cert.gov	Third Party Advi
[R2] Advantech WebAccess Stack Buffer Overflow - Research Advisory Tenable®	MISC	www.tenable.com	Third Party Advi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)