

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA Advantech WebAccess

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-480>

Gestion du document

Référence	CERTA-2013-AVI-480
Titre	Vulnérabilité dans le système SCADA Advantech WebAccess
Date de la première version	19 août 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité ICS-CERT du 13 août 2013
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque(s)

– injection de code indirecte à distance

2 Systèmes affectés

Advantech WebAccess version 7.0 et antérieures

3 Résumé

Une vulnérabilité a été corrigée dans *Advantech WebAccess*. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS).

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletins de sécurité Advantech
<http://webaccess.advantech.com/security.php>
- Bulletin de sécurité ICS-CERT du 13 août 2013
<http://ics-cert.us-cert.gov/advisories/ICSA-13-225-01>
- Référence CVE CVE-2013-2299
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2299>

Gestion détaillée du document

19 août 2013 version initiale.