

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le système SCADA Schneider Electric TAC I/A

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-2012-AVI-575>

Gestion du document

Référence	CERTA-2012-AVI-575
Titre	Vulnérabilités dans le système SCADA Schneider Electric TAC I/A
Date de la première version	16 octobre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Scheider Electric du 17 août 2012
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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Versions antérieures à Schneider Electric TAC I/A Series 3G 3.6.47 pour la branche 3.6
- Versions antérieures à Schneider Electric TAC I/A Series 3G 3.5.39

3 Résumé

Quatre vulnérabilités ont été corrigées dans les systèmes SCADA *Schneider Electric TAC I/A*. Elles concernent, un accès arbitraire aux fichiers, le stockage des mots de passe, un système de *cookie* faible et des identifiants de sessions prédictibles.

4 Solution

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

5 Documentation

- Bulletin de sécurité Scheider Electric du 17 août 2012:
http://download.schneider-electric.com/files?p_File_Id=25785825&p_File_Name=TAC--I-A-Series-G3-Vulnerability-Disclosure_SEVD-12-230-0_17.08.2012.pdf

Gestion détaillée du document

16 octobre 2012 version initiale.