

Vulnérabilité dans Schneider Electric Accutech Manager (SCADA)

Référence : CERT-IST/AV-2013.128
Version : 1.0
Date de la version : 13 Février 2013

Classification de la vulnérabilité

Risque : ■ Très élevé
Conséquence : Prise de contrôle du système
Niveau de connaissance de l'attaquant : Connaisseur
Moyen nécessaire à l'attaquant : A distance sans compte via un service annexe

Information sur le(s) système(s) impacté(s)

Plate(s)-forme(s) impactée(s) :

- Systèmes Microsoft Windows

Logiciel(s) impacté(s) :

- Accutech Manager versions 2.00.1 et précédentes

Liste exhaustive des produits du catalogue Cert-IST impactés :

Description

Contexte de publication :

Cette vulnérabilité possédait la référence **FA-2013.0023** dans la liste des failles en cours d'investigation du Cert-IST.

Nature du problème :

Une vulnérabilité a été découverte dans l'application Accutech Manager de Schneider Electric . Elle permet à une personne malveillante de provoquer un déni de service voire de prendre à distance le contrôle total d'un système vulnérable.

Nota : Un code d'exploitation de cette vulnérabilité a été publié sur Internet.

Contexte technique :

Accutech Manager est un composant de gestion utilisé dans un système de surveillance basé sur des sondes. Il est utilisé par des applications pour lesquelles des données provenant de sondes distantes sont récoltées, surveillées, affichées ou archivées.

Analyse détaillée :

Cette vulnérabilité est due à un débordement de mémoire qui peut se produire lors du traitement de requêtes de grande taille de type GET. Elle permet à un attaquant distant, via du trafic réseau vers le port TCP 2537, de provoquer l'arrêt de l'application ou d'exécuter du code arbitraire sur le système avec les privilèges administrateur.

Solution

Mettre à jour Accutech Manager vers la version 2.00.2 ou ultérieure

Aucun

- Mises à jour des produits Schneider Electric Accutech
 - <http://www.schneider-electric.com/download/ww/en/results/0/1555898-Software--Released/28460036-Accutech/>

Note(s) CVSS

- Cert-IST - CERT-IST/AV-2013.128
 - Base score : 10.0 - AV:A/AC:L/Au:N/C:I/C/A:C
 - Score temporaire : 8.3 - AV:A/AC:L/Au:N/C:I/C/A:C/E:F/RL:OF/RC:C

Identifiant(s) du problème

- CVE: [CVE-2013-0658](#)

Documentation additionnelle

- Avis de sécurité de Schneider Electric SEVD 2013-021-01 du 21 janvier 2013
 - <http://www.schneider-electric.com/download/ww/en/details/35974865-Vulnerability-Disclosure-for-Accutech-Manager-SW/>
- Avis de sécurité de l'ICS-CERT ICSA-13-043-01 du 12 février 2013
 - <http://ics-cert.us-cert.gov/pdf/ICSA-13-043-01.pdf>

Version	Commentaire	Date
---------	-------------	------

Version	Commentaire	Date
1.0	Création de l'avis	13/02/2013