Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 21 mai 2013
N° CERTA-2013-AVI-318

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA Schneider

Gestion du document

Référence	CERTA-2013-AVI-318
Titre	Vulnérabilité dans le système SCADA Schneider
Date de la première version	21 mai 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Schneider du 20 mai 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)

– exécution de code arbitraire à distance

2 Systèmes affectés

– CitectFacilities versions 7.10 et antérieures
– CitectSCADA versions 7.0 et antérieures

3 Résumé

Une vulnérabilité a été corrigée dans *Mitsubishi MX Component*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 Solution

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

5 Documentation

- Guide sur la cybersécurité des systèmes industriels
  http://www.ssi.gouv.fr/systemesindustriels
- Bulletin de sécurité Schneider du 20 mai 2013
  http://www.citect.schneider-electric.com/index.php?option=com_content&view=article&id=1728&Itemid=1789
- Référence CVE CVE-2013-3075
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3075

Gestion détaillée du document

21 mai 2013 version initiale.