

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA MOXA OnCell Gateway

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-462>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2013-AVI-462 |
| Titre | Vulnérabilité dans le système SCADA MOXA OnCell Gateway |
| Date de la première version | 07 août 2013 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité ICS-CERT du 06 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)

- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 Systèmes affectés

- Moxa OnCell Gateway G3111
- Moxa OnCell Gateway G3151
- Moxa OnCell Gateway G3211
- Moxa OnCell Gateway G3251

3 Résumé

Une vulnérabilité a été corrigée dans *MOXA OnCell Gateway*. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.

4 Solution

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

5 Documentation

- Bulletin de sécurité ICS-CERT du 06 août 2013
<http://ics-cert.us-cert.gov/advisories/ICSA-13-217-01>
- Lien de téléchargement du firmware
http://www.moxa.com/support/sarch_result.aspx?type=soft&prod_id=316&type_id=4
- Référence CVE CVE-2012-3039
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3039>

Gestion détaillée du document

07 août 2013 version initiale.