

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA les produits Siemens

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTFR-2016-AVI-196 |
| Titre | Multiples vulnérabilités dans SCADA les produits Siemens |
| Date de la première version | 10 juin 2016 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité SCADA Siemens SSA-526760 du 08 juin 2016 Bulletin de sécurité SCADA Siemens SSA-818183 du 08 juin 2016 |
| 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)

- déni de service à distance
- contournement de la politique de sécurité

2 - Systèmes affectés

- Siemens SIMATIC WinCC flexible versions antérieures à 2008 SP3 Up7
- Siemens SIMATIC S7-300 versions antérieures à V3.2.12
- Siemens SIMATIC S7-300 versions V3.3.x antérieures à V3.3.12

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *SCADA les produits Siemens*. Elles permettent à un attaquant de provoquer un déni de service à distance et un contournement de la politique de sécurité.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité SCADA Siemens SSA-526760 du 08 juin 2016
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-526760.pdf
- Bulletin de sécurité SCADA Siemens SSA-818183 du 08 juin 2016
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-818183.pdf
- Référence CVE CVE-2015-1358
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1358>
- Référence CVE CVE-2016-3949
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3949>

Gestion détaillée du document

10 juin 2016 version initiale.

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-196>
