

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA les produits Siemens

Gestion du document

Référence	CERTFR-2017-AVI-200
Titre	Multiples vulnérabilités dans SCADA les produits Siemens
Date de la première version	05 juillet 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-452237 du 04 juillet 2017 Bulletin de sécurité Siemens SSA-323211 du 04 juillet 2017
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
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Module Ethernet EN100 pour SIPROTEC 4 et SIPROTEC Compact sans le dernier correctif de sécurité
- Module Ethernet EN100 pour Reyrolle sans le dernier correctif de sécurité

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, un contournement de la politique de sécurité 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 Siemens SSA-452237 du 04 juillet 2017
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-452237.pdf
- Bulletin de sécurité Siemens SSA-323211 du 04 juillet 2017
https://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-323211.pdf
- Référence CVE CVE-2015-5374
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5374>
- Référence CVE CVE-2016-4784
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4784>
- Référence CVE CVE-2016-4785
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4785>
- Référence CVE CVE-2016-7112
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7112>
- Référence CVE CVE-2016-7113
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7113>
- Référence CVE CVE-2016-7114
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7114>

Gestion détaillée du document

05 juillet 2017 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-2017-AVI-200>
