

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans SCADA les produits Siemens

Gestion du document

Référence	CERTFR-2016-AVI-250
Titre	Multiples vulnérabilités dans SCADA les produits Siemens
Date de la première version	25 juillet 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité SCADA SSA-378531 Siemens du 22 juillet 2016 Bulletin de sécurité SCADA SSA-119132 Siemens du 22 juillet 2016 Bulletin de sécurité SCADA SSA-453276 Siemens du 22 juillet 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)

- exécution de code arbitraire à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- injection de code indirecte à distance
- déni de service à distance

2 - Systèmes affectés

- Siemens WinCC V7.3 sans la mise à jour de sécurité U10
- Siemens WinCC V7.4 sans la mise à jour de sécurité U1
- Siemens PCS 7 V8.1 SP1 avec WinCC V7.3 sans la mise à jour de sécurité U10, SIMATIC BATCH V8.1 SP1 sans la mise à jour de sécurité U9, OpenPCS 7 V8.1 sans la mise à jour de sécurité U3
- Siemens PCS 7 V8.2 avec WinCC V7.4 sans la mise à jour de sécurité U1, OpenPCS 7 V8.2 sans la mise à jour de sécurité U3
- Siemens WinCC Runtime Professional V13 versions antérieures à WinCC Runtime Professional V13 SP1 U9
- Siemens SINEMA Remote Connect Server versions antérieures à 1.2
- Siemens SIMATIC NET PC-Software versions antérieures à V13 SP2

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *SCADA les produits Siemens*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire 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 SCADA SSA-378531 Siemens du 22 juillet 2016
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-378531.pdf
- Bulletin de sécurité SCADA SSA-119132 Siemens du 22 juillet 2016
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-119132.pdf
- Bulletin de sécurité SCADA SSA-453276 Siemens du 22 juillet 2016
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_SSA-453276.pdf
- Référence CVE CVE-2016-5743
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5743>
- Référence CVE CVE-2016-5744
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5744>
- Référence CVE CVE-2016-6204
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6204>
- Référence CVE CVE-2016-5874
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5874>

Gestion détaillée du document

25 juillet 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-250
