

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans les systèmes SCADA Siemens

### Gestion du document

Référence	CERTFR-2015-AVI-022
Titre	Multiples vulnérabilités dans les systèmes SCADA Siemens
Date de la première version	14 janvier 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-311299 du 13 janvier 2015
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)

- contournement de la politique de sécurité
- élévation de privilèges

### 2 - Systèmes affectés

- SIMATIC WinCC Sm@rtClient for iOS versions antérieures à V1.0.2
- SIMATIC WinCC Sm@rtClient Lite for iOS versions antérieures à V1.0.2

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans les systèmes SCADA *Siemens*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une élévation de privilèges.

### 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-311299 du 13 janvier 2015  
[http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-311299.pdf](http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-311299.pdf)
- Référence CVE CVE-2014-5231  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5231>
- Référence CVE CVE-2014-5232  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5232>
- Référence CVE CVE-2014-5233  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5233>

## Gestion détaillée du document

**14 janvier 2015** 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-2015-AVI-022>

---