

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans le système SCADA Siemens WinCC

---

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-457>

---

### Gestion du document

Référence	CERTA-2013-AVI-457
Titre	Multiples vulnérabilités dans le système SCADA Siemens WinCC
Date de la première version	01 août 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-064884 du 31 juillet 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)

- injection de code indirecte à distance
- injection de requêtes illégitimes par rebond

## 2 Systèmes affectés

- Siemens WinCC version 11
- Siemens WinCC version 12 antérieures à SP1

## 3 Résumé

De multiples vulnérabilités ont été corrigées dans le système SCADA *Siemens WinCC*. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et une injection de requêtes illégitimes par rebond (CSRF).

## 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-064884 du 31 juillet 2013  
[http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-064884.pdf](http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-064884.pdf)
- Référence CVE CVE-2013-4911  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4911>
- Référence CVE CVE-2013-4912  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4912>

### **Gestion détaillée du document**

**01 août 2013** version initiale.