

Affaire suivie par :  
CERTA

## AVIS DU CERTA

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

### Gestion du document

Référence	CERTA-2013-AVI-676
Titre	Multiples vulnérabilités dans les systèmes SCADA Siemens
Date de la première version	13 décembre 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens SSA-742938 du 04 décembre 2013 Bulletin de sécurité Siemens SSA-324789 du 06 décembre 2013 Bulletin de sécurité Siemens SSA-568732 du 06 décembre 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)

- contournement de la politique de sécurité
- élévation de privilèges

### 2 - Systèmes affectés

- Siemens SINAMICS S/G versions antérieures à 4.6.11
- Siemens RuggedCom versions antérieures à 3.12.2
- Siemens COMOS versions antérieures à 9.2.0.8.1
- Siemens COMOS versions antérieures à 10.0.3.1.40
- Siemens COMOS versions antérieures à 10.1.0.0.2

### 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-742938 du 04 décembre 2013  
[http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-742938.pdf](http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-742938.pdf)
- Bulletin de sécurité Siemens SSA-324789 du 06 décembre 2013  
[http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-324789.pdf](http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-324789.pdf)
- Bulletin de sécurité Siemens SSA-568732 du 06 décembre 2013  
[http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens\\_security\\_advisory\\_ssa-568732.pdf](http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-568732.pdf)
- Référence CVE CVE-2013-6840  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6840>
- Référence CVE CVE-2013-6920  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6920>
- Référence CVE CVE-2013-6925  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6925>
- Référence CVE CVE-2013-6926  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6926>

## Gestion détaillée du document

13 décembre 2013 version initiale.

---

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-676>

---