

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA Siemens Simatic RF Manager

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-026>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2013-AVI-026 |
| Titre | Vulnérabilité dans le système SCADA Siemens Simatic RF Manager |
| Date de la première version | 15 janvier 2013 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Siemens ssa-099741 du 14 janvier 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- RF-MANAGER 2008
- RF-MANAGER Basic version 3.0 et antérieures

3 Résumé

Une vulnérabilité a été corrigée dans *Siemens Simatic RF Manager*. Elle concerne un débordement de mémoire tampon dans l'*ActiveX*. Un utilisateur malintentionné peut alors faire exécuter à une cible du code arbitraire à distance au moyen d'une page Web spécialement conçue.

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-099741 du 14 janvier 2013 :
http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-099741.pdf
- Guide de sécurité des systèmes industriels :
<http://www.ssi.gouv.fr/systemsindustriels>

Gestion détaillée du document

15 janvier 2013 version initiale.