

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA Siemens SiPass Server

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-2012-AVI-632>

Gestion du document

Référence	CERTA-2012-AVI-632
Titre	Vulnérabilité dans le système SCADA Siemens SiPass Server
Date de la première version	08 novembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens ssa-938777 du 08 octobre 2012
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

Siemens SiPass Server intégrant MP2.6 et versions antérieures

3 Résumé

Une vulnérabilité critique a été corrigée dans *Siemens SiPass Server*. Elle permet à un attaquant d'exécuter du code arbitraire à distance au moyen de messages spécialement conçus.

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-938777 du 08 octobre 2012
http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-938777.pdf

Gestion détaillée du document

08 novembre 2012 version initiale.