Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 14 septembre 2012
N° CERTA-2012-AVI-507

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans système SCADA Siemens WinCC

Gestion du document

Référence	CERTA-2012-AVI-507
Titre	Multiples vulnérabilités dans système SCADA Siemens WinCC
Date de la première version	14 septembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Siemens ssa-864051 du 10 septembre 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

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

2 Systèmes affectés

WinCC version 7.0 SP3 et antérieures.

3 Résumé

Cinq vulnérabilités ont été corrigées dans le système SCADA *Siemens WinCC*. Parmis elles :
- deux concernent des injections de code indirecte à distance (XSS) ;
- une permet de récupérer des données d'autres utilisateurs ;
- une concerne une injection de type SQL ;
- la dernière permet d'obtenir l'identifiant et le mot de passe d'un utilisateur au moyen d'un *ActiveX*.

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-864051 du 10 septembre 2012 :
  http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-864051.pdf
- Référence CVE CVE-2012-3034 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3034
- Référence CVE CVE-2012-3032 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3032
- Référence CVE CVE-2012-3031 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3031
- Référence CVE CVE-2012-3030 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3030
- Référence CVE CVE-2012-3028 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3028

Gestion détaillée du document

14 septembre 2012 version initiale.