Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 octobre 2012
N° CERTA-2012-AVI-574

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le système SCADA Schneider Electric Critical Power and Cooling Services

Gestion du document

Référence	CERTA-2012-AVI-574
Titre	Vulnérabilité dans le système SCADA Schneider Electric Critical Power and Cooling Services
Date de la première version	16 octobre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Schneider Electric du 17 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Network Management Card (NMC) Device IP Wizard (Java Version 7)
- Netbotz Advanced View (Java Version 6)
- PowerChute Network Shutdown (Java Version 6)
- PowerChute Business Edition (Java Version 6)
- StruxureWare Data Center Expert (Java Version 6)
- StruxureWare Operations (Java Version 6)

3 Résumé

Une vulnérabilité critique a été corrigée dans *Schneider Electric Critical Power and Cooling Services* (CPCS). Elle permet à un attaquant d'exécuter du code arbitraire à distance en utilisant un "applet" Java spécialement conçu. La vulnérabilité concerne la *Java Runtime Environment* (JRE) et permet de contourner les restrictions du "SecurityManager".

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Schneider Electric du 17 septembre 2012 :
  http://www2.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/162000/FA162073/en_US/
  2012-4681)%20Advisory.pdf
- Référence CVE CVE-2012-4681 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4681

Gestion détaillée du document

16 octobre 2012 version initiale.