Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 février 2009
N° CERTA-2009-AVI-052

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du système SCADA e-terrahabitat d'AREVA

Gestion du document

Référence	CERTA-2009-AVI-052
Titre	Multiples vulnérabilités du système SCADA e-terrahabitat d'AREVA
Date de la première version	06 février 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'US-CERT numéro VU#337569 du 05 février 2009
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 ;
- déni de service à distance ;
- élévation de privilèges.

2 Systèmes affectés

- AREVA e-terrahabitat version 5.7 et versions antérieures.

3 Résumé

De multiples vulnérabilités ont été découvertes dans le système de gestion d'énergie `e-terraplatform` d'`AREVA`. L'exploitation de ces vulnérabilités permet de réaliser, entre autre, une exécution de code arbitraire à distance ou un déni de service à distance.

4 Description

Cinq vulnérabilités ont été découvertes dans le système de gestion d'énergie `e-terraplatform` d'`AREVA` :

- la première permet d'exécuter du code arbitraire à distance via un dépassement de mémoire ;
- trois autres vulnérabilités présentes au niveau des applications `WebFGServer` et `NETIO` permettent de réaliser un déni de service à distance ;
- la dernière vulnérabilité située au niveau de l'application `WebFGServer` permet à un utilisateur malveillant d'élever ses privilèges.

5 Solution

Contacter le support de l'application afin d'obtenir la mise à jour *e-terrahabitat_560_P20081030_SEC.patch*.

6 Documentation

- Site de l'éditeur :
  http://www.areva.com
- Note de vulnérabilité de l'US-CERT VU#337569 du 05 février 2009 :
  http://www.kb.cert.org/vuls/id/337569
- Référence CVE CVE-2009-0210 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0210
- Référence CVE CVE-2009-0211 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0211
- Référence CVE CVE-2009-0212 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0212
- Référence CVE CVE-2009-0213 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0213
- Référence CVE CVE-2009-0214 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0214

Gestion détaillée du document

05 février 2009 version initiale.