

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les produits Citect

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-2008-AVI-312>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2008-AVI-312 |
| Titre | Vulnérabilité dans les produits Citect |
| Date de la première version | 13 juin 2008 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Core Security CORE-2008-0125 du 11 juin 2008 |
| 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.

2 Systèmes affectés

- CitectFacilities 7.x ;
- CitectSCADA 6.x ;
- CitectSCADA 7.x.

3 Résumé

Une vulnérabilité affectant les produits *Citect* permet à une personne malveillante d'exécuter du code arbitraire ou d'effectuer un déni de service à distance.

4 Description

Les produits *Citect* offrent une interface de contrôle et de collecte d'information pour des équipements industriels. Une vulnérabilité due à une erreur dans un composant du serveur *ODBC* permet à une personne distante d'effectuer un déni de service ou une exécution de code arbitraire via un paquet spécialement conçu. Le port par défaut en écoute de cette application est *20222/TCP*.

5 Solution

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

6 Documentation

- Bulletin de sécurité Core Security CORE-2008-0125 du 11 juin 2008 :
<http://www.coresecurity.com/?action=item&id=2186>
- Référence CVE CVE-2008-2639 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2639>

Gestion détaillée du document

13 juin 2008 version initiale.