



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2007
N° CERTA-2007-AVI-367

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ESRI ArcSDE

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-2007-AVI-367>

Gestion du document

Référence	CERTA-2007-AVI-367
Titre	Vulnérabilité dans ESRI ArcSDE
Date de la première version	17 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense 577 du 15 août 2007
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

- Les versions de ESRI ArcSDE antérieures à 9.2 Service Pack 3.

3 Résumé

Une vulnérabilité a été identifiée dans ESRI ArcSDE. L'exploitation de cette dernière permettrait à une personne malveillante de perturber le service, donc d'empêcher les utilisateurs d'accéder au serveur, voire d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été identifiée dans ESRI ArcSDE (*Advanced Spatial Data Server*). Cette technologie est intégrée dans ArcGIS Server pour accéder aux bases de données géographiques multi-utilisateurs GIS (*Geographical Information Systems*).

La vulnérabilité est un débordement de tampon, exploitable à distance par des entrées particulières au format ASCII de l'utilisateur. Les conséquences d'une telle exploitation seraient la perturbation du service, voire l'exécution de code arbitraire à distance.

Par défaut, le serveur est en écoute sur le port 5151/TCP.

5 Solution

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

6 Documentation

- Bulletin de sécurité iDefense du 15 août 2007 :
<http://labs.idefense.com/intelligence/vulnerabilities/display?id=577>
- Référence CVE CVE-2007-4278 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4278>
- Page officielle du produit ESRI ArcSDE :
<http://www.esri.com/software/arcgis/arcscde/index.html>
- Détails des correctifs effectués pour ESRI ArcSDE 9.2 Service Pack 3 :
http://download.esri.com/support/downloads/other_/ArcSDE-92sp3-issues.htm

Gestion détaillée du document

17 août 2007 version initiale.