



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mai 2006
N° CERTA-2006-AVI-207

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Sun Java System Server et Sun ONE Server

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-2006-AVI-207>

Gestion du document

Référence	CERTA-2006-AVI-207
Titre	Vulnérabilité de Sun Java System Server et Sun ONE Server
Date de la première version	19 mai 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Sun
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

- Sun Java System Web Server version 6.1 Service Pack 4 et les versions antérieures ;
- Sun Java System Application Server version 7 2004Q2 Standard Edition Update 2 et les versions antérieures ;
- Sun Java System Application Server version 7 2004Q2 Enterprise Edition Update 2 et les versions antérieures ;
- Sun ONE Web Server 6.0 Service Pack 9 et les versions antérieures ;
- Sun ONE Application Server 7 Platform Edition Update 6 et les versions antérieures ;
- Sun ONE Application Server 7 Standard Edition Update 6 et les versions antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans certaines versions de Sun Java System Server et Sun ONE Server. Elle permet à un utilisateur malveillant utilisant une technique d'injection de code indirecte (ou *Cross-Site Scripting*) pour exécuter du code arbitraire à distance sur une machine se connectant au serveur.

4 Description

Une vulnérabilité a été identifiée dans certaines versions de Sun Java System Server et Sun ONE Server. Ceux-ci ne vérifient pas correctement certaines adresses réticulaires (ou URI pour *Universal Resource Identifier*) retournées dans une page d'erreur et contenant le caractère guillemet ". Un utilisateur malveillant peut utiliser cette vulnérabilité en injectant une URI spéciale dans un serveur. Ceci représente une attaque par injection de code arbitraire (ou *Cross-Site Scripting*) : du code arbitraire peut être exécuté sur la machine d'un utilisateur qui visite la page d'erreur sur le site où le serveur Sun fonctionne.

5 Solution

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

6 Documentation

- Bulletin de mise à jour Java System Web Server version 6.1 :
<http://www.sun.com/download/products.xml?id=434aec1d>
- Bulletin de mise à jour Sun Java System Application Server version 7 2004Q2 Standard Edition :
<http://www.sun.com/download/products.xml?id=427fe06d>
- Bulletin de mise à jour Sun Java System Application Server version 7 2004Q2 Enterprise Edition :
<http://javashoplmsun.com>
- Bulletin de mise à jour Sun ONE Web Server 6.0 :
<http://www.sun.com/download/products.xml?id=43a84f89>
- Bulletin de mise à jour Sun ONE Application Server 7 Platform Edition :
<http://www.sun.com/download/products.xml?id=42ae3178>
- Bulletin de mise à jour Sun ONE Application Server 7 Standard Edition :
<http://www.sun.com/download/products.xml?id=42ae317c>

Gestion détaillée du document

19 mai 2006 version initiale.