Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 novembre 2001
N° CERTA-2001-AVI-150

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur Xsun sous Solaris

Gestion du document

Référence	CERTA-2001-AVI-150
Titre	Vulnérabilité du serveur Xsun sous Solaris
Date de la première version	26 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin Sun Alert Notification #26359
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 avec les privilèges de l'administrateur `root`.

2 Systèmes affectés

Solaris 8 et version antérieures.

3 Résumé

Une vulnérabilité présente dans le serveur Xsun permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

4 Description

Xsun est un serveur X démarré sur les stations de travail utilisant l'environnement graphique X11.

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

Cette vulnérabilité n'est exploitable qu'en local.

5 Contournement provisoire

Selon SUN, une solution de contournement provisoire consiste à changer les permissions de l'exécutable au moyen de la commande suivante: `chmod 0755 /usr/openwin/bin/Xsun`.

Réaliser cette modification empêche le démarrage du serveur Xsun par les commandes telles que `openwin` et `xinit`. Il convient donc de s'assurer que le démarrage du serveur X est réalisé au moyen des gestionnaires d'environnement graphique tels que `xdm` ou `dtlogin`.

6 Solution

Des correctifs sont disponibles. Se référer au bulletin de sécurité de SUN (cf. section Documentation).

7 Documentation

Bulletin Sun Alert Notification #26359 disponible à l'adresse suivante:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=salert%2F26359&&wholewords=on

Gestion détaillée du document

26 novembre 2001 version initiale.