



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2004
N° CERTA-2002-AVI-253-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de XFS (XWindow Font 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-2002-AVI-253>

Gestion du document

Référence	CERTA-2002-AVI-253-004
Titre	Vulnérabilité de XFS (XWindow Font Server)
Date de la première version	27 novembre 2002
Date de la dernière version	20 janvier 2004
Source(s)	Avis de sécurité CA-2002-34 du CERT/CC
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.

2 Systèmes affectés

- Solaris versions 2.5.1 à 9 ;
- SGI IRIX version 6.5.13 et antérieures ;
- HP-UX 10.10, 10.20, 10.24, 11.00, 11.04, 11.11 et 11.22 ;
- IBM AIX 4.3, 5.1 et 5.2.

3 Résumé

Une vulnérabilité du service `xfs` permet à un utilisateur mal intentionné d'exécuter du code arbitraire, à distance, sur la machine vulnérable.

4 Description

Le serveur `xfs` (XWindow Font Serveur) est utilisé sur les serveurs X Window pour distribuer les polices de caractères aux clients X Window.

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter, à distance, du code arbitraire sur la machine vulnérable.

5 Contournement provisoire

Filtrer au niveau du pare-feu le port 7100/tcp utilisé par `xfs` afin d'empêcher l'exploitation de cette vulnérabilité depuis l'Internet.

6 Solution

Se référer aux bulletins de sécurité des différents éditeurs pour l'obtention des correctifs.

7 Documentation

- Avis de sécurité "Solaris fs.auto Remote Compromise Vulnerability" d'ISS :
<http://bvlive01.iss.net/issEN/delivery/xforce/alertdetail.jsp?oid=21541>
- Avis de sécurité "Buffer Overflow Vulnerability in X Font Server" de SGI :
<ftp://patches.sgi.com/support/free/security/advisories/20021202-01-I>
- Avis de sécurité CA-2002-34 du CERT/CC :
<http://www.cert.org/Advisories/CA-2002-34.html>
- Bulletin de sécurité #48879 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/48879>
- Bulletin de sécurité HPSBUX0212-228 de Hewlett-Packard :
<http://itrc.hp.com>
- Bulletin de sécurité IBM AIX :
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1601.1>
- Référence CVE CAN-2002-1317 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1317>

Gestion détaillée du document

27 novembre 2002 version initiale.

28 novembre 2002 ajout référence au bulletin de sécurité #48879 de Sun.

05 décembre 2002 suppression des mentions spécifiques à Solaris, ajout référence au bulletin de sécurité de SGI.

10 décembre 2002 ajout référence au bulletin de sécurité HPSBUX0212-228 de Hewlett-Packard.

20 janvier 2004 ajout bulletin IBM et référence CVE.