

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités de X Window sous SGI Irix

---

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-236>

---

### Gestion du document

Référence	CERTA-2002-AVI-236
Titre	Multiples vulnérabilités de X Window sous SGI Irix
Date de la première version	21 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité #20021001-01-P de SGI
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

- Elévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

SGI Irix 6.5.

## 3 Résumé

Plusieurs vulnérabilités de différents outils de X Window permettent de bloquer le serveur X ou d'obtenir les privilèges de l'administrateur `root` sous SGI Irix 6.5.

## 4 Description

De multiples vulnérabilités de X Window permettent à un utilisateur mal intentionné d'obtenir les privilèges de l'administrateur `root` ou d'arrêter le serveur X.

- Il est possible d'utiliser une vulnérabilité des bibliothèques `zlib` décrite dans l'avis CERTA-2002-AVI-052 sous X Window pour exécuter du code arbitraire avec les privilèges de l'administrateur `root`.
- Une vulnérabilité de la gestion des feuilles de style par le logiciel Mozilla (navigateur, messagerie) versions 1.0 et antérieures peut entraîner un dysfonctionnement des utilitaires sous X Window ou de bloquer le serveur X.  
Un utilisateur mal intentionné peut ainsi effectuer un déni de service en propageant un document (sur un site web, par mél, ou de toute autre façon) utilisant une feuille de style astucieusement construite.
- MIT-SHM (MIT SHared Memory) est un outil permettant d'accélérer les capacités graphiques ou d'améliorer le traitement de certaines images.  
Une vulnérabilité de MIT-SHM sous X window permet à un utilisateur local mal intentionné d'avoir accès en lecture et écriture à des segments de mémoire partagée.

## 5 Contournement provisoire

- Si cela est possible, désactiver X Window au moyen de la commande `/usr/gfx/stopgfx`.
- Utiliser la version la plus récente possible de Mozilla.

## 6 Solution

Consulter le bulletin de sécurité de SGI (voir le paragraphe documentation) pour connaître la disponibilité des correctifs.

## 7 Documentation

- Bulletin de sécurité #20021001-01-P de SGI :  
<ftp://patches.sgi.com/support/free/security/advisories/20021001-01-P>
- Avis de sécurité du CERTA concernant les bibliothèques `zlib` CERTA-2002-AVI-052 : « Vulnérabilité dans la bibliothèque `zlib` / `libz` »

## Gestion détaillée du document

21 octobre 2002 version initiale.