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-151

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Xview sous Solaris

Gestion du document

Référence	CERTA-2001-AVI-151
Titre	Vulnérabilité de Xview sous Solaris
Date de la première version	26 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Elévation de privilèges
- Exécution de code arbitraire en local avec les privilèges de l'utilisateur `root`.

2 Systèmes affectés

- Solaris 2.4, 2.5, 2.5.1, 2.6 pour SPARC et Intel ;
- Solaris 7 pour Sparc, sans le correctif 107374-02 ;
- Solaris 8 pour Sparc, sans le correctif 111626-01 ;
- Solaris 7 pour Intel sans le correctif 107375-02 ;
- et Solaris 8 pour Intel sans le correctif 111627-01.

3 Résumé

Il est possible d'obtenir en local les privilèges de l'utilisateur propriétaire d'une application liée à `Xview` grâce à un débordement de mémoire de cette librairie.

4 Description

`Xview` est une librairie graphique pour l'interface graphique (GUI) *Open Look*.

Toute application ayant les drapeaux positionnés `SUID` ou `GUID` et utilisant cette librairie permet d'exécuter du code arbitraire avec les permissions du compte propriétaire de l'application.

De plus, si le propriétaire de l'application est l'utilisateur `root`, ce débordement de mémoire permet d'obtenir les privilèges de l'administrateur de la machine..

5 Contournement provisoire

Rechercher les applications liées à la librairie `Xview` au moyen de la commande `ldd`. Si une ligne contenant `libxview.so` apparait, l'application est liée à Xview.

Vérifier qu'elles ne sont pas `SUID` ou `GUID` par la commande `ls -l`. Si un 's' apparaît dans la liste des permissions pour l'utilisateur ou le groupe, alors cette application est `S/GUID`.

Supprimer le bit `SUID` ou `GUID` de l'application à l'aide de la commande `chmod`.

ATTENTION : Ce contournement provisoire ne protège pas le système contre le débordement de mémoire. Il faut donc enlever le bit `SUID` ou `GUID` à toute autre application liée à `Xview` ajoutée ultérieurement.

6 Solution

Pour les systèmes 7 et 8, appliquer le correctif selon la verion :

- Pour Sparc :
  - Solaris 7 : correctif numéro 107374-02 ;
  - Solaris 8 : correctif numéro 111626-01.
- Sur Intel :
  - Solaris 7 : correctif numéro 107375-02 ;
  - Solaris 8 : correctif numéro 111627-01.

Ces correctifs sont disponibles sur le site de Sun :
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

7 Documentation

Bulletin de sécurité Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=salert%2F27513&&wholewords=on

Gestion détaillée du document

26 novembre 2001 version initiale.