Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 janvier 2003
N° CERTA-2003-AVI-007

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de utmp_update sous Solaris

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-2003-AVI-007

Gestion du document

Référence	CERTA-2003-AVI-007
Titre	Vulnérabilité de utmp_update sous Solaris
Date de la première version	21 janvier 2003
Date de la dernière version	–
Source(s)	Bulletin d'alerte #50008 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

- Elévation de privilèges ;
- exécution de code arbitraire.

Cette vulnérabilité n'est pas exploitable à distance.

2 Systèmes affectés

- Solaris 2.6 sous architecture i386 et Sparc ;
- Solaris 7 sous architecture i386 et Sparc ;
- Solaris 8 sous architecture i386 et Sparc ;
- Solaris 9 sous architecture i386 et Sparc.

`Nota` : La vulnérabilité n'a pas été vérifiée par Sun sur la version 2.5.1 de Solaris, et Sun indique qu'il ne développera pas de correctif pour ce système.

3 Résumé

Un débordement de mémoire de la fonction `utmp_update` sous Solaris permet d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

4 Description

Le programme `utmp_update` présent dans le répertoire `/usr/lib` est une fonction non documentée appelée par le système pour mettre à jour les enregistrements des fichiers `utmp` et `utmpx`.

Ces derniers journalisent les connexions des utilisateurs au système et sont accessibles par des programmes tels que `who`, `login`, `last`, etc.

Un utilisateur mal intentionné peut exécuter du code arbitraire avec les privilèges de l'administrateur `root` au moyen d'un débordement de mémoire de la fonction `utmp_update`.

Il faut être connecté localement pour pouvoir exploiter cette vulnérabilité.

5 Solution

Consulter le bulletin d'alerte #50008 de Sun (voir paragraphe Documentation) pour connaître la disponibilité des correctifs à appliquer.

6 Documentation

Bulletin de sécurité #50008 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50008

Gestion détaillée du document

21 janvier 2003 version initiale.