Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 octobre 2002
N° CERTA-2002-AVI-241

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du logiciel Web-Based Enterprise Management sous Solaris 8

Gestion du document

Référence	CERTA-2002-AVI-241
Titre	Vulnérabilité du logiciel Web-Based Enterprise Management sous Solaris 8
Date de la première version	31 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin d'alerte #48320 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 ou déni de service exploitable localement.

2 Systèmes affectés

Sun Solaris 8.

3 Résumé

Solaris 8 update 1/01 installe par défaut des paquetages de Web-Based Enterprise Management dont les fichiers sont accessibles en écriture par tous les utilisateurs du système.

4 Description

Dans sa version 1/01, Solaris 8 installe par défaut les paquetages de Web-Based Enterprise Management suivants :

– SUNWwbdoc ;

– SUNWwbcou ;
– SUNWwbdev ;
– SUNWmgapp.

Ces paquetages installent des fichiers qui sont accessibles en écriture par tous les utilisateurs du système.
Un utilisateur mal intentionné connecté localement peut modifier ces fichiers de façon à obtenir les privilèges de l'administrateur `root` ou effectuer un déni de service..

5 Contournement provisoire

Ces fichiers sont situés dans le répertoire `/usr/sadm` et `/usr/demo/wbem` et ont les permissions en écriture (`w`) pour leur `groupe` d'appartenance et pour `tous` (*group* et *other*).
Supprimer le bit écriture de tous ces fichiers à l'aide de la commande `chmod`.

6 Solution

– Se référer au bulletin d'alerte #48320 de Sun (voir paragraphe documentation) pour connaître la disponibilité des correctifs.
– La version 9 de Solaris corrige cette vulnérabilité.

7 Documentation

Bulletin d'alerte #48320 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F48320

Gestion détaillée du document

31 octobre 2002 version initiale.