Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juin 2002
N° CERTA-2002-AVI-125

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des services snmpd et edd sur la console SSP (SUN Enterprise 10000)

Gestion du document

Référence	CERTA-2002-AVI-125
Titre	Vulnérabilité des services snmpd et edd sur la console SSP (SUN Enterprise 10000)
Date de la première version	13 juin 2002
Date de la dernière version	–
Source(s)	Bulletin Sun Alert Notification #43985
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.

2 Systèmes affectés

System Service Processor (SSP) versions 3.5 et antérieures.

3 Résumé

Une vulnérabilité de type débordement de mémoire présente dans les services `snmpd` et `edd` permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`.

4 Description

Le System Service Processor (SSP) est un ensemble logiciel et matériel (basé sur une station de travail SUN Solaris) permettant d'administrer les systèmes SUN Enterprise 10000.

Des tests effectués par l'université finlandaise d'Oulu ont mis en évidence la présence de vulnérabilités dans les routines de décodage et de traitement des messages SNMP dans de nombreuses implémentations (se référer au bulletin d'alerte CERTA-2002-ALE-004 du CERTA).

Selon SUN, les services `snmpd` et `edd` de la console SPP font partie des implémentations vulnérables.

5 Contournement provisoire

Installer la console SPP sur un réseau dédié.

Note : le service `snmpd` est un agent SNMP mandataire s'appuyant sur le service `machine_server` pour l'allocation des ports. Le filtrage du port 161/udp utilisé par le protocole SNMP V1 au niveau du garde-barrière n'est donc pas suffisant.

6 Solution

Se référer au bulletin de sécurité de SUN (cf. section Documentation) pour la disponibilité des correctifs.

7 Documentation

- Bulletin Sun Alert Notification #43985 disponible à l'adresse suivante :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F43985&zone_32=category%3Asecurity
- Documentation "Sun Enterprise 10000 SSP User guide" :
  http://www.sun.com/products-n-solutions/hardware/docs/806-4871-10.pdf

Gestion détaillée du document

13 juin 2002 version initiale.