Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 avril 2002
N° CERTA-2002-AVI-069-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités des agents SNMP sous 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-069

Gestion du document

Référence	CERTA-2002-AVI-069-001
Titre	Vulnérabilités des agents SNMP sous IRIX
Date de la première version	04 avril 2002
Date de la dernière version	25 avril 2002
Source(s)	Avis 20020201-01-P de SGI Avis 20020404-01-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

IRIX 6.5 à 6.5.15 (première vulnérabilité).
IRIX 6.5 à 6.5.16 (deuxième vulnérabilité).
Les versions antérieures, non maintenues, n'ont pas été testées.

3 Résumé

Un utilisateur mal intentionné peut utiliser une vulnérabilité de l'agent SNMP sous IRIX pour exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

Le sous-agent SNMP HP-UX MIB (`hpsnmpd`) est également vulnérable.

4 Description

Les 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).

4.1 Première vulnérabilité

Une vulnérabilité de l'agent SNMP (exécutables `/usr/etc/snmpd`, `/usr/etc/peer_snmpd` et `/usr/etc/peer_enca` livrés avec le paquetage `eoe.sw.netman`) permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur `root`. Cette vulnérabilité, de type débordement de mémoire, est exploitable à distance.

4.2 Deuxième vulnérabilité

Grâce à des paquets habilement constitués, un utilisateur mal intentionné peut forcer, à distance, l'arrêt du sous-agent SNMP HP-UX MIB (exécutable `/usr/etc/hpsnmpd`).

Le sous-agent SNMP HP-UX MIB (paquetage `snmpd.sw.hp`) n'est pas installé par défaut.

5 Contournement provisoire

- Ne démarrer le service SNMP que si celui-ci est nécessaire. Dans le cas contraire, les paquetages `eoe.sw.netman` et texttsnmpd.sw.hp peuvent être désinstallés par la commande suivante : `versions remove eoe.sw.netman snmpd.sw.hp` ;
- filtrer le port 161/udp utilisé par le protocole SNMP V1 au niveau du garde-barrière afin d'empêcher l'exploitation de cette vulnérabilité depuis l'Internet.

6 Solution

La version 6.5.16 d'IRIX corrige la première vulnérabilité.

Pour ces deux vulnérabilités, des correctifs sont disponibles sur le site du constructeur (se référer à la section Documentation).

7 Documentation

- Avis de sécurité 20020201-01-P de SGI disponible à l'adresse suivante :
  ftp://patches.sgi.com/support/free/security/advisories/20020201-01-P
- Avis de sécurité 20020404-01-P de SGI disponible à l'adresse suivante :
  ftp://patches.sgi.com/support/free/security/advisories/20020404-01-P

Gestion détaillée du document

04 avril 2002 version initiale.

25 avril 2002 Prise en compte de l'avis 20020404-01-P relatif à hpsnmpd.