

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service nsd 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-089>

Gestion du document

Référence	CERTA-2002-AVI-089
Titre	Vulnérabilité du service nsd sous IRIX
Date de la première version	02 mai 2002
Date de la dernière version	–
Source(s)	Avis 20020501-01-I 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

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

IRIX 6.5 à 6.5.10.

Les versions antérieures, non maintenues, n'ont pas été testées.

3 Résumé

En exploitant une vulnérabilité du daemon nsd, un utilisateur local peut corrompre n'importe quel fichier du système.

4 Description

Le daemon `nsd` (Unified Name Service Daemon) met en cache des informations relatives aux utilisateurs, groupes et machines, en puisant dans les fichiers de configuration locaux et en interrogeant les serveurs NIS, NIS+, LDAP, DNS sur le réseau.

`nsd` est installé par défaut sur toutes les versions 6.5.x d'Irix.

A la réception du signal `USR1`, `nsd` écrit dans le fichier `/usr/tmp/nsd` sans vérifier l'identité du propriétaire de ce fichier. Un utilisateur mal intentionné peut ainsi créer un lien symbolique nommé `/usr/tmp/nsd.dump` pointant sur n'importe quel fichier du système pour le corrompre.

5 Solution

La version 6.5.11 d'IRIX corrige cette vulnérabilité.

6 Documentation

Avis de sécurité 20020501-01-I de SGI disponible à l'adresse suivante :
<ftp://patches.sgi.com/support/free/security/advisories/20020501-01-I>

Gestion détaillée du document

02 mai 2002 version initiale.