

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans talkd

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-109>

Gestion du document

Référence	CERTA-2002-AVI-109-001
Titre	Vulnérabilité dans talkd
Date de la première version	23 mai 2002
Date de la dernière version	12 juin 2002
Source(s)	Alerte de sécurité #44646 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.

2 Systèmes affectés

- talkd sous Solaris 2.5.1 et 2.6 ;
- talkd sous Redhat Linux antérieure à la version 6.0 ;
- talkd sous OpenBSD antérieure à la version 2.8 ;
- talkd Système IRIX versions 6.5.9 et antérieures (les versions antérieures, non maintenues, n'ont pas été testées).

3 Résumé

Une vulnérabilité de type « chaîne de format » présente dans le daemon talkd permet à un utilisateur distant d'obtenir les privilèges du super utilisateur du système (root).

4 Description

Le service `talk` permet de dialoguer en temps réel à travers le réseau. C'est une application de type client/serveur.

Une vulnérabilité présente sur le serveur `talkd` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du super utilisateur par l'envoi d'un message malicieusement construit. Cette vulnérabilité est présente lorsque un appel est effectuée d'un client vers le serveur.

5 Contournement provisoire

Désactiver le daemon `talkd`.

6 Solution

Appliquer le correctif correspondant à votre système d'exploitation (se référer à la section documentation).

7 Documentation

Alerte de Sécurité #1764 de Sun :

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2f44646>

Site de SecurityFocus :

<http://online.securityfocus.com/bid/1764>

Avis de sécurité de SGI :

<http://www.sgi.com/support/security/>

Gestion détaillée du document

23 mai 2002 version initiale.

12 juin 2002 Ajout de l'avis de sécurité Irix.