

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans telnetd

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-2001-AVI-081>

Gestion du document

Référence	CERTA-2001-AVI-081-003
Titre	Débordement de mémoire dans telnetd
Date de la première version	25 juillet 2001
Date de la dernière version	11 juin 2002
Source(s)	Avis CA-2001-21 du CERT/CC Avis de sécurité FreeBSD-SA-01:49 Avis de sécurité SGI 20010801-01-P Avis de sécurité de différentes distributions Linux Bulletin de sécurité M-006 du CIAC Bulletin d'alerte Sun #28063
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

Exécution de code arbitraire avec les privilèges du *daemon* telnetd (le plus souvent root) à distance.
Des programmes exploitant cette vulnérabilité ont été diffusés sur l'Internet.

2 Systèmes affectés

Tous les serveurs de connexion telnet, dont les sources sont issues de la version BSD (FreeBSD, OpenBSD, Windows NT, SGI Irix, IBM Aix, Linux Debian, Mandrake, RedHat, HP-UX...).

3 Résumé

Un utilisateur mal intentionné peut exécuter à distance, et sans authentification préalable, du code arbitraire avec les privilèges de l'utilisateur propriétaire du *daemon* telnetd.

4 Description

Une vulnérabilité dans le traitement des options du protocole telnet (fonction `telrcv`) permet à un utilisateur mal intentionné d'exécuter à distance, et sans authentification préalable, du code arbitraire sur le serveur telnet au moyen d'un débordement de mémoire dans cette fonction.

Nota : Le *daemon* `telnetd` est installé et lancé par défaut sur les systèmes FreeBSD entre autres.

Nota : Sur certaines distributions de Linux (Mandrake, RedHat, Debian ...), le service `telnet` est installé avec le paquetage `netkit`.

5 Contournement provisoire

- Si le service `telnet` n'est pas utilisé sur une machine, ou s'il est temporairement impossible d'installer le correctif il faut arrêter `telnetd` et l'empêcher de redémarrer.
Il est généralement lancé par le biais d'`inetd` ou `xinetd`.
- Dans la mesure du possible, le propriétaire d'un service tel que `telnet` ne doit pas être `root`.
- Restreindre l'accès au service `telnet` au niveau des gardes-barrières (le port standard pour le service `telnet` est 23/TCP).

6 Solution

Se référer aux bulletins de sécurité des différents distributeurs pour appliquer les correctifs (Cf. paragraphe Documentation).

7 Documentation

- Avis CA-2001-21 du CERT/CC :
<http://www.cert.org/advisories/CA-2001-21.html>
- Bulletin de sécurité du CIAC :
<http://www.ciac.org/ciac/bulletins/m-006.shtml>
- Avis de sécurité FreeBSD-SA-01:49 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:49.telnetd.asc>
- Bulletin de sécurité SGI :
<http://patches.sgi.com/support/free/security/advisories/20010801-01-P>
- Bulletin de sécurité Debian concernant `netkit-telnet` :
<http://www.debian.org/security/2001/dsa-070>
- Bulletin d'alerte #28063 de Sun :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F28063>

Gestion détaillée du document

25 juillet 2001 version initiale.

24 août 2001 seconde version : ajout des correctifs concernant les principales distributions Unix dans la rubrique Solution et modification du titre de l'avis.

19 octobre 2001 troisième version : Ajout d'informations concernant HP-UX.

11 juin 2002 quatrième version : Ajout du bulletin d'alerte de Sun dans le paragraphe Documentation, reformulation du paragraphe Solution.