

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans le client Telnet

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-2005-AVI-124>

Gestion du document

Référence	CERTA-2005-AVI-124-005
Titre	Multiples vulnérabilités dans le client Telnet
Date de la première version	30 mars 2005
Date de la dernière version	22 juillet 2005
Source(s)	Bulletin de sécurité US-CERT VU#291924 du 28 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

Client Telnet.

3 Résumé

Deux vulnérabilités découvertes dans le client Telnet permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

Le client Telnet permet d'émuler un terminal à distance.

Deux vulnérabilités de type débordement de mémoire peuvent être exploitées au travers des fonctions `slc_add_reply()` et `env_opt_add()`. Ces vulnérabilités permettent à un individu mal intentionné d'exécuter du code arbitraire à distance, au moyen de réponses malicieusement constituées.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité 220 d'iDefense du 28 mars 2005 :
<http://www.iddefense.com/application/poi/display?id=220&type=vulnerabilities>
- Bulletin de sécurité 221 d'iDefense du 28 mars 2005 :
<http://www.iddefense.com/application/poi/display?id=221&type=vulnerabilities>
- Bulletin de sécurité US-CERT VU#291924 du 28 mars 2005 :
<http://www.kb.cert.org/vuls/id/291924>
- Bulletin de sécurité MIT krb5 Security Advisory 2005-001 du 28 mars 2005 :
<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2005-001-telnet.txt>
- Bulletin de sécurité Debian DSA-697 du 29 mars 2005 :
<http://www.debian.org/security/2005/dsa-697>
- Bulletin de sécurité Debian DSA-699 du 29 mars 2005 :
<http://www.debian.org/security/2005/dsa-699>
- Bulletin de sécurité Debian DSA-731 du 02 juin 2005 :
<http://www.debian.org/security/2005/dsa-731>
- Bulletin de sécurité Gentoo GLSA-200504-04 / telnet du 06 avril 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200504-04.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:061 du 29 mars 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:061>
- Bulletin de sécurité RedHat RHSA-2005:327-10 du 28 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-327.html>
- Bulletin de sécurité RedHat RHSA-2005:330-06 du 30 mars 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-330.html>
- Bulletin de sécurité SuSE SUSE-SR:2005:009 du 29 mars 2005 :
http://www.novell.com/linux/security/advisories/2005_09_sr.html
- Mise à jour de sécurité pour Fedora Core 2 du 30 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité pour Fedora Core 3 du 30 mars 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité FreeBSD SA-05:01.telnet du 28 mars 2005 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:01.telnet.asc>
- Bulletin de sécurité OpenBSD pour telnet du 30 mars 2005 :
<http://www.openbsd.org/errata.html#telnet>
- Bulletin de sécurité SUN #57755 du 29 mars 2005 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1>
- Bulletin de sécurité Avaya ASA-2005-132 du 14 juin 2005 :
http://support.avaya.com/elmodocs2/security/ASA-2005-132_RHSA-2005-327.pdf
- Bulletin de sécurité Debian DSA-765 du 22 juillet 2005 :
<http://www.debian.org/security/2005/dsa-765>
- Référence CVE CAN-2005-0468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0468>
- Référence CVE CAN-2005-0469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0469>

Gestion détaillée du document

30 mars 2005 version initiale.

31 mars 2005 ajout de la référence au bulletin de sécurité OpenBSD.

13 mars 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA-200504-04.

02 juin 2005 ajout de la référence au bulletin de sécurité Debian DSA-731.

17 juin 2005 ajout du bulletin de sécurité Avaya ASA-2005-132.

22 juillet 2005 ajout de la référence au bulletin de sécurité Debian DSA-765.