

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des bibliothèques libtasn1 et GnuTLS

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-2006-AVI-081>

Gestion du document

Référence	CERTA-2006-AVI-081-001
Titre	Vulnérabilité des bibliothèques libtasn1 et GnuTLS
Date de la première version	17 février 2006
Date de la dernière version	08 mars 2006
Source(s)	
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 potentielle de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Tout système utilisant les bibliothèques :

- libtasn1 dans une version source antérieure à la 0.2.18 ;
- GnuTLS dans une version source antérieure à la 1.2.10 (stable) ou 1.3.4 (développement).

3 Résumé

Une faille dans la bibliothèque libtasn1 (nativement incluse dans GnuTLS) permet à un utilisateur distant mal intentionné de provoquer un déni de service – voire l'exécution de code –, à l'aide d'un certificat volontairement mal formé, de toute application réseau utilisant la bibliothèque GnuTLS.

4 Description

GnuTLS est bibliothèque permettant d'ajouter le support des sessions TLS/SSLv3 à des applications réseaux. Le décodage des certificats X509 est confié à la bibliothèque `libtasn1` qui est vulnérable à un débordement de tampon.

Parmi les produits utilisant GnuTLS, on trouve le serveur de messagerie Exim, le client de messagerie instantanée Gaim, le système d'accès aux fichiers du bureau Gnome via `gnome-vfs`, le lecteur multimedia VLC, le serveur d'impression CUPS,...

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation) ou mettre à jour les sources :

- `libtasn1` en version 0.2.18 au moins ;
- GnuTLS en versions 1.2.10 (stable) ou 1.3.4 (développement) au moins.

A l'issue redémarrer les services utilisant GnuTLS.

6 Documentation

- Site internet de GnuTLS :
<http://www.gnu.org/software/gnutls/>
- Mise à jour de sécurité Fedora Core 4 du 10 février 2006 :
<http://www.redhat.com/archives/fedora-announce-list/2006-February/msg00043.html>
- Bulletin de sécurité Gentoo GLSA-200602-08 du 16 février 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200602-08.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:029 du 13 février 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:029>
- Bulletin de sécurité RedHat RHSA-2006:0207 du 10 février 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0207.html>
- Bulletin de sécurité Ubuntu USN-251-1 du 16 février 2006 :
<http://www.ubuntulinux.org/usn/usn-251-1>
- Bulletin de sécurité Debian DSA-985 du 06 mars 2006 :
<http://www.debian.org/security/2006/dsa-985>
- Bulletin de sécurité Debian DSA-986 du 06 mars 2006 :
<http://www.debian.org/security/2006/dsa-986>
- Référence CVE CAN-2006-0645 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0645>

Gestion détaillée du document

17 février 2006 version initiale.

08 mars 2006 ajout des références aux bulletins de sécurité Debian.