

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du système de réseau privé virtuel OpenVPN

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-435>

Gestion du document

Référence	CERTA-2005-AVI-435-002
Titre	Vulnérabilité du système de réseau privé virtuel OpenVPN
Date de la première version	03 novembre 2005
Date de la dernière version	09 novembre 2005
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

- Déni de service en mode serveur,
- exécution de code arbitraire à distance en mode client.

2 Systèmes affectés

- OpenVPN versions 2.0 antérieures à la 2.0.4 :
- pour les versions Unix en mode client,
 - pour les versions Unix comme Windows en mode serveur.

3 Résumé

Deux vulnérabilités ont été identifiées dans le code d'OpenVPN. L'une permet d'exécuter du arbitraire sur un client se connectant à un serveur malicieux.

4 Description

OpenVPN est une solution de réseau privé virtuel, existant pour Unix et Windows, et utilisant SSL/TLS pour assurer la phase d'authentification.

Une vulnérabilité dans une chaîne de format peut être utilisée pour exécuter du code arbitraire sur une station cliente se connectant à un serveur volontairement malicieux ou préalablement compromis (CVE-2005-3393).

Une faille dans le mode serveur avec transport TCP peut provoquer l'arrêt du serveur lors d'une connexion (CVE-2005-3409).

5 Solution

Se reporter au bulletin de l'éditeur pour l'obtention des correctifs (cf. Documentation) ou mettre à jour les sources en version 2.0.4 au moins.

6 Documentation

- Site internet d'OpenVPN :
<http://openvpn.net>
- Bulletin de sécurité FreeBSD du 01 novembre 2005 :
<http://www.vuxml.org/freebsd/pkg-openvpn.html>
- Bulletin de sécurité Gentoo GLSA 200511-07.xml du 06 novembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200511-07.xml>
- Bulletin de sécurité Debian DSA-885 du 07 novembre 2005 :
<http://www.debian.org/security/2005/dsa-885>
- Bulletin de sécurité Mandriva MDKSA-2005:206 du 08 novembre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:206>
- Bulletin de sécurité SUSE SUSE-SR:2005:025 du 04 novembre 2005 :
<http://lists.suse.com/archive/suse-security-announce/2005-Nov/0001.html>
- Référence CVE CVE-2005-3393 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3393>
- Référence CVE CVE-2005-3409 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3409>

Gestion détaillée du document

03 novembre 2005 version initiale.

08 novembre 2005 ajout des références aux bulletins de sécurité Gentoo, Debian et SUSE.

09 novembre 2005 ajout de la référence au bulletin de sécurité Mandriva MDKSA-2005:206.