



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 05 mars 2012
N° CERTA-2011-AVI-465-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans stunnel

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-2011-AVI-465>

Gestion du document

Référence	CERTA-2011-AVI-465-001
Titre	Vulnérabilité dans stunnel
Date de la première version	23 août 2011
Date de la dernière version	05 mars 2012
Source(s)	Notes de version stunnel 4.42
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 à distance ;
- déni de service à distance.

2 Systèmes affectés

stunnel versions antérieures à 4.42.

3 Résumé

Une vulnérabilité permettant de provoquer un déni de service et potentiellement de l'exécution de code arbitraire à distance a été corrigée dans stunnel.

4 Description

Une vulnérabilité de type corruption de mémoire a été corrigée dans stunnel. Cette vulnérabilité peut être utilisée par une personne distante malintentionnée pour provoquer un déni de service ou de l'exécution de code arbitraire.

5 Solution

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

6 Documentation

- Notes de version stunnel 4.42 :
<http://www.stunnel.org/pipermail/stunnel-announce/2011-August/00059.html>
- Bulletin de sécurité Gentoo GLSA 201202-08 du 29 février 2012 :
<http://www.gentoo.org/security/en/glsa/glsa-201202-08.xml>
- Référence CVE CVE-2011-2940 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2940>

Gestion détaillée du document

23 août 2011 version initiale ;

05 mars 2012 ajout du bulletin de sécurité Gentoo.