



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 mai 2012
N° CERTA-2012-AVI-281

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Socat

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-2012-AVI-281>

Gestion du document

Référence	CERTA-2012-AVI-281
Titre	Vulnérabilité dans Socat
Date de la première version	16 mai 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Socat du 14 mai 2012
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.

2 Systèmes affectés

- Socat version 1.4.0.0 à 1.7.2.0 ;
- socat version 2.0.0-b1 à 2.0.0-b4.

3 Résumé

Une vulnérabilité a été corrigée dans *Socat*. Elle est présente lors de l'utilisation de l'option « READLINE » et provoque un débordement de mémoire tampon dans le tas. Une exploitation réussie de cette faille peut mener à une exécution de code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Socat du 14 mai 2012 :
<http://www.dest-unreach.org/socat/contrib/socat-secadv3.html>
- Référence CVE CVE-2012-0219 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0219>

Gestion détaillée du document

16 mai 2012 version initiale.