Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 janvier 2006
N° CERTA-2006-AVI-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabiliés sur SCPonly

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-001

Gestion du document

Référence	CERTA-2006-AVI-001
Titre	Vulnérabiliés sur SCPonly
Date de la première version	02 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo
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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- scponly versions 3.x ;
- scponly versions 4.x antérieures à la version 4.2.

3 Résumé

Deux vulnérabilités présentes sur `scponly` peuvent être exploitées par un utilisateur mal intentionné pour contourner la politique de sécurité ou pour élever ses privilèges sur le système.

4 Description

L'application `scponly` est une application basée sur Openssh dont le but est de restreindre les utilisateurs à employer uniquement la commande `scp`.

– La première vulnérabilité est présente dans le binaire `scponlyc`, elle permet à un utilisateur local mal intentionné d'élever ses privilèges sur la machine hébergeant l'application vulnérable.
– La seconde vulnérabilité permet à un utilisateur distant mal intentionné, via des arguments passés en ligne de commande, de contourner la politique de sécurité mise en place par scponly afin de pouvoir exécuter des commandes sur le système.

5 Contournement provisoire

6 Solution

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

7 Documentation

– Site Internet de scponly :
http://www.sublimation.org/scponly
– Bulletin de sécurité Gentoo GLSA-200512-17 du 17 décembre 2005 :
http://www.gentoo.org/security/en/glsa/glsa-200512-17.xml
– Bulletin de sécurité de FreeBSD du 22 décembre 2005 :
http://www.vuxml.org/freebsd/index.html

Gestion détaillée du document

02 janvier 2006 version initiale.