Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2005
N° CERTA-2005-AVI-083-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans PuTTY

Gestion du document

Référence	CERTA-2005-AVI-083-001
Titre	Vulnérabilité dans PuTTY
Date de la première version	21 février 2005
Date de la dernière version	22 février 2005
Source(s)	Bulletins de sécurité de l'éditeur du 20 février 2005
Pièce(s) jointe(s)	

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire.

2 Systèmes affectés

PuTTY 0.x.

3 Résumé

Deux vulnérabilités présentes dans le logiciel PuTTY permet à un individu mal intentionné d'exécuter du code arbitraire à distance avec les droits de l'utilisateur ayant démarré PuTTY.

4 Description

PuTTY est une mise en œuvre libre de Telnet et SSH pour les plates-formes Windows et Linux.

Deux vulnérabilités de type débordement d'entier (`integer overflow`) présente dans la fonction `fxp_readdir_recv()` et dans la fonction `sftp_pkt_getstring()` permettent à un utilisateur mal intentionné, via un serveur `SFTP` (SSH File Tranfer Protocol) qui retourne des réponses malicieusement construites d'exécuter du code arbitraire à distance sur le système vulnérable.

5 Solution

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

6 Documentation

- Annonce de sécurité "PuTTY vulnérability vuln-sftp-readdir" du 20 février 2005 : http://www.chiark.greenend.org.uk/ sgtatham/putty/wishlist/vuln-sftp-readdir.html
- Annonce de sécurité "PuTTY vulnérability vuln-sftp-string" du 20 février 2005 : http://www.chiark.greenend.org.uk/ sgtatham/putty/wishlist/vuln-sftp-string.html
- Bulletin de sécurité Gentoo GLSA 200502-28 / PuTTY du 21 février 2005 : http://www.gentoo.org/security/en/glsa/glsa-200502-28.xml
- Bulletin de sécurité FreeBSD pour PuTTY du 20 février 2005 : http://www.vuxml.org/freebsd/
- Mise à jour disponible : http://www.chiark.greenend.org.uk/ sgtatham/putty/download.html

Gestion détaillée du document

21 février 2005 version initiale.
22 février 2005 ajout des références aux bulletins de sécurité Gentoo et FreeBSD.