



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2002
N° CERTA-2002-AVI-204

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de PGP

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-2002-AVI-204>

Gestion du document

Référence	CERTA-2002-AVI-204
Titre	Vulnérabilité de PGP
Date de la première version	09 septembre 2002
Date de la dernière version	–
Source(s)	Avis de sécurité de Foundstone Labs
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 ;
- divulgation du mot de passe associé à la clé privée PGP.

2 Systèmes affectés

PGP Corporate Desktop 7.1.1 sur Windows 2000 et XP.

3 Résumé

Une vulnérabilité de PGP de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, et de récupérer le mot de passe associé à la clé privée de la victime.

4 Description

Dans les fonctions de chiffrement et de déchiffrement d'un fichier, il est possible d'exploiter une vulnérabilité de type débordement de mémoire en utilisant un nom de fichier trop long.

Un utilisateur mal intentionné peut ainsi chiffrer un message habilement conçu et le faire déchiffrer par la victime. Il lui est alors possible d'exécuter des commandes sur la machine cible, et de récupérer le mot de passe associé à la clé privée de la victime. En effet, le débordement de mémoire a lieu juste après le déchiffrement du fichier, et avant l'effacement de la mémoire contenant le mot de passe.

5 Solution

Appliquer le correctif publié par NAI (cf. section Documentation).

6 Documentation

- Avis de sécurité 090502-PCRO de Foundstone Labs :
<http://www.foundstone.com/knowledge/randd-advisories-display.html?id=334>
- Correctif de NAI :
<http://www.nai.com/naicommon/download/upgrade/patches/patch-pgphotfix.asp>

Gestion détaillée du document

09 septembre 2002 version initiale.