Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 décembre 2001
N° CERTA-2001-AVI-164

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur pfinger

Gestion du document

Référence	CERTA-2001-AVI-164
Titre	Vulnérabilité du serveur pfinger
Date de la première version	20 décembre 2001
Date de la dernière version	–
Source(s)	INTEXXIA
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.

2 Systèmes affectés

- client `pfinger` ;
- serveur esclave `pfinger`.

Les versions du logiciel antérieures à la version 0.7.8 sont affectées. `pfinger` est un logiciel qui tourne sur UNIX ou ses variantes.

3 Résumé

Le logiciel finger possède des vulnérabilités qui autorisent dans certaines conditions l'exécution de code arbitraire.

4 Description

Le protocole finger (cf. **?**) permet d'accéder à des informations nominatives sur les utilisateurs connectés à un ordinateur. Chaque utilisateur peut personnaliser les informations nominatives délivrées par le protocole finger en créant un fichier `~/.plan`.

Le logiciel `pfinger` est un serveur qui met en œuvre ce protocole.

Une vulnérabilité basée sur l'usage des « chaînes de format » permet à un utilisateur mal intentionné de construire un fichier `.plan` particulier sur la machine qui héberge le serveur `finger`. Lorsque les informations contenues dans le fichier sont affichées par le client `pfinger`, il est possible que du code arbitraire placé dans le fichier `.plan` s'exécute sur la machine qui héberge le client.

Une vulnérabilité analogue affecte les serveurs `pfinger`. Lorsqu'un serveur « esclave » `pfinger` reçoit des informations d'un serveur maître, il est possible que dans certaines conditions il reçoive du serveur maître du code à exécuter.

En principe `pfinger` s'exécute en ayant les droits de l'utilisateur `nobody`. Cet utilisateur n'a pas beaucoup de droits. Toutefois en combinant avec d'autres vulnérabilités locales, il pourrait être possible dans certains cas d'obtenir des privilèges plus élevés.

5 Solution

5.1 pfinger

Un correctif existe à partir de la version 0.7.8 de `pfinger` sur le site **?**.

5.2 le protocole finger

Les failles dans `pfinger` permettent de s'attaquer à ceux qui consultent les informations nominatives. Toutefois, il convient de rappeler que, indépendamment de la faille sur ce logiciel, le protocole finger est par nature un protocole dangereux. La nature des informations délivrées peut nuire au serveur qui les publie. Depuis des années ce protocole est connu comme pouvant servir de préparation à des attaques en aidant à la collecte d'informations sur la victime. C'est pourquoi dans un environnement hostile, Internet par exemple, il est souhaitable de ne pas utiliser ce protocole, c'est à dire s'assurer que la la ligne suivante dans le fichier `/etc/inetd.conf` est commentée (elle doit commencer par le caractère « # ») :

```
#finger         stream  tcp     nowait  nobody  /usr/sbin/tcpd  /usr/sbin/in.fingerd
```

On peut aussi appliquer une politique de filtrage au niveau du garde barrière en interdisant les requêtes sur le port `79/tcp`.

Gestion détaillée du document

20 décembre 2001 version initiale.