Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2001
N° CERTA-2001-AVI-095

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des *daemons* `smap/smapd` (ou `CSMAP`)

Gestion du document

Référence	CERTA-2001-AVI-095
Titre	Vulnérabilité des *daemons* `smap/smapd` (ou `CSMAP`)
Date de la première version	13 septembre 2001
Date de la dernière version	–
Source(s)	Avis CA-2001-25 du CERT/CC
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 sur le garde-barrière avec les privilèges du *daemon* `smap/smapd`.

2 Systèmes affectés

Tous les systèmes sur lesquels sont installés le *daemon* `smap/smapd` (ou `CSMAP` sur certains systèmes). Parmis ceux ci :

- Gauntlet Firewall versions 5.x pour Unix ;
- PGP e-ppliance série 300 version 1.0, 1.5, 2.0 ;
- PGP e-ppliance séries 100 et 120 ;
- PGP e-ppliance série 300 versions 1,5 et 2,0 ;
- PGP e-ppliance série 1000 versions 1,5 et 2,0 ;
- MacAfee Webshield pour Solaris 4.1 ;
- MacAfee e-ppliance séries 100 et 120 ;

D'autres systèmes peuvent être affectés. Contactez votre distributeur.

D'après l'éditeur de M-Wall, les versions 4.5 et 4.0 ne sont pas vulnérables.

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire à distance avec les privilèges des *daemons* `smap/smapd` (ou `CSMAP`).

4 Description

`smap/smapd` (ou `CSMAP`) est un service permettant le transfert de courrier à travers des systèmes tels que des garde-barrières.

Grâce à un débordement de mémoire du service `smap/smapd` (ou `CSMAP`), un utilisateur mal intentionné peut exécuter du code arbitraire à distance avec les privilèges de ce service.

5 Contournement provisoire

Désactiver ce *daemon* si vous ne l'utilisez pas.

6 Solution

Appliquer le correctif selon le système :

- Pour les produits PGP :
  http://www.pgp.com/naicommon/download/upgrade/upgrade-patch.asp
- Pour les produits NAI :
  ftp://www.nai.com/security

7 Documentation

- Bulletin de sécurité du CERT/CC :
  http://www.cert.org/advisories/CA-2001-25.html
- Le bulletin de sécurité de PGP :
  http://www.pgp.com/support/product-advisories/csmap.asp

Gestion détaillée du document

13 septembre 2001 version initiale.