Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 avril 2004
N° CERTA-2004-AVI-132-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans SSMTP

Gestion du document

Référence	CERTA-2004-AVI-132-001
Titre	Vulnérabilités dans SSMTP
Date de la première version	16 avril 2004
Date de la dernière version	27 avril 2004
Source(s)	Avis de sécurité Debian
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 à distance ;
- déni de service.

2 Systèmes affectés

`SSMTP 2.x`.

3 Résumé

Deux vulnérabilités présentes dans le paquetage `SSMTP 2.x` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou de réaliser un déni de service à distance.

4 Description

Deux vulnérabilités de type chaîne de format sont présentes dans les fonctions `die()` et `log_event()` dans le paquetage `SSMTP`.

Un utilisateur mal intentionné peut, via une chaîne malicieusement construite dans certains paramètres, réaliser un déni de service ou exécuter du code arbitraire sur le système ayant une version de `SSMTP` vulnérable.

5 Solution

Appliquer le correctif (cf. section documentation).

6 Documentation

- Référence CVE CAN-2004-0156 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0156
- Avis de sécurité Debian :
  http://www.debian.org/security/2004/dsa-485
- Bulletin de sécurité de Gentoo :
  http://security.gentoo.org/glsa/glsa-200404-18.xml

Gestion détaillée du document

16 avril 2004 version initiale.
27 avril 2004 ajout référence au bulletin de sécurité de Gentoo.