

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Sendmail

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-140>

Gestion du document

Référence	CERTA-2002-AVI-140
Titre	Vulnérabilité dans Sendmail
Date de la première version	28 juin 2002
Date de la dernière version	–
Source(s)	Site Internet de Sendmail
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 ;
- déni de service.

2 Systèmes affectés

Toutes les versions de Sendmail antérieures à la version 8.12.5.

3 Résumé

Un débordement de mémoire peut aboutir à l'exécution de code arbitraire ou à un déni de service.

4 Description

Sendmail est une application permettant l'envoi de courrier électronique sur l'Internet. Selon la configuration de cette application, un utilisateur mal intentionné peut exécuter du code arbitraire sur le serveur avec les privilèges de l'utilisateur ayant lancé le service (généralement `root`). Ceci peut conduire à un déni de service. Cette

vulnérabilité ne peut se produire que si le service Sendmail est configuré pour utiliser une table DNS au format TXT et si l'utilisateur mal intentionné contrôle un serveur DNS.

5 Solution

La version 8.12.5 de Sendmail corrige cette vulnérabilité. Elle est disponible en téléchargement sur le site web de Sendmail (cf. Documentation).

6 Documentation

Site Internet de Sendmail :
<http://www.sendmail.org/>

Gestion détaillée du document

28 juin 2002 version initiale.