Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 octobre 2001
N° CERTA-2001-AVI-106

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Sendmail

Gestion du document

Référence	CERTA-2001-AVI-106
Titre	Multiples vulnérabilités dans Sendmail
Date de la première version	02 octobre 2001
Date de la dernière version	–
Source(s)	Avis de sécurité Razor : "Multiple local sendmail vulnerabilities"
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

- Elévation de privilèges;
- lecture, modification des méls;
- supression de méls.

Les vulnérabilités ne sont pas exploitables à distance.

2 Systèmes affectés

La vulnérabilité permettant la supression des méls est présente dans la version sendmail 8.12.0 et les versions antérieures.

Seule la version 8.12.0 est concernée par l'élévation de privilèges et la lecture/modification des méls des utilisateurs.

3 Résumé

De multiples vulnérabilités présentes dans sendmail permettent à un utilisateur mal intentionné de réaliser une élévation de privilèges ou de manipuler les files d'attente de méls.

4 Description

Une vulnérabilité dans la routine de traitement des fichiers et des paramètres de configuration de sendmail permet à un utilisateur mal intentionné d'obtenir des privilèges lui permettant de manipuler les files d'attente de méls (lecture, supression, modification de messages) et dans certains cas obtenir les privilèges de l'administrateur (`root`) sur la machine.

Cette vulnérabilité n'est présente que dans la version 8.12.0 de sendmail.

Une autre vulnérabilité, présente dans les version 8.12.0 et antérieures, permet à un utilisateur mal intentionné de spécifier des options lors du traitement de la file d'attente des méls (`sendmail -q`). Des options judicieusement choisies permettent de supprimer des méls ou de réaliser un déni de service.

Les systèmes n'autorisant pas le parcours de la file d'attente par un utilisateur non privilégié (option `RestrictQRun`) ne sont pas vulnérables (cette option n'est pas positionnée par défaut).

5 Solution

La version 8.12.1 de sendmail corrige ces vulnérabilités.
Elle est disponible sur le site de sendmail :
http://www.sendmail.org/8.12.1.html

6 Documentation

Avis de sécurité Razor : "Multiple local sendmail vulnerabilities"

Gestion détaillée du document

02 octobre 2001 version initiale.