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 juin 2001
N° CERTA-2001-AVI-070

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Exim

Gestion du document

Référence	CERTA-2001-AVI-070
Titre	Vulnérabilité dans Exim
Date de la première version	27 juin 2001
Date de la dernière version	–
Source(s)	Avis de sécurité RedHat RHSA-2001:078-05
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

Obtention du privilège root à distance.

2 Systèmes affectés

Version de Exim antérieures ou égales à la version 3.22

3 Résumé

Sous certaines conditions, un utilisateur mal intentionné peut exécuter du code arbitraire à distance.

4 Description

Exim est un routeur de mail (Message Transfert Agent) qui peut remplacer sendmail, postfix...
Une erreur dans le code vérifiant les en-tête de méls, permet à un utilisateur mal intentionné d'exécuter un code arbitraire.
Cette vulnérabilité est exploitable seulement si Exim est configuré pour tester les en-têtes de méls.

5 Contournement provisoire

Ne pas positionner la directive `headers_check_syntax` dans le fichier de configuration d'Exim.

6 Solution

Télécharger le correctif disponible sur le site de RedHat :

- ftp://updates.redhat.com/6.2/powertools/i386/exim-3.22-6x.i386.rpm
- ftp://updates.redhat.com/7.0/powertools/i386/exim-3.22-13.i386.rpm
- ftp://updates.redhat.com/7.1/powertools/i386/exim-3.22-6x.i386.rpm

Télécharger le correctif disponible sur le site de Debian :

- http://security.debian.org/dists/stable/updates/main/binary-i386/exim_3.12-10.1_i386.db

7 Documentation

Le site Exim:
http://www.exim.org

Gestion détaillée du document

27 juin 2001 version initiale.