Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 mai 2004
N° CERTA-2004-AVI-157-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Exim

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-157

Gestion du document

Référence	CERTA-2004-AVI-157-003
Titre	Vulnérabilités dans Exim
Date de la première version	07 mai 2004
Date de la dernière version	17 mai 2004
Source(s)	Avis de sécurité #68 de Georgi Guninski
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.

2 Systèmes affectés

- Exim 3.35 ;
- exim 4.32 (pour certaines vulnérabilités).

3 Résumé

Georgi Guninski a découvert deux vulnérabilités affectant certaines versions d'`exim`.

4 Description

Exim est un routeur de mail (Message Transfert Agent) fonctionnant sous Linux. Deux vulnérabilités ont été découvertes dans exim :

- Un défaut de vérification des adresses de l'émetteur des messages électroniques permet l'exploitation d'un débordement de tampon afin d'exécuter du code arbitraire. L'exploitation de cette vulnérabilité nécessite le

positionnement du paramètre `sender_verify` à `true`. Cette vulnérabilité n'affecte pas la version 4.32 d'exim.

– une vulnérabilité est présente dans la mise en œuvre de la vérification de la syntaxe de l'entête d'un message éléctronique. Celle-ci peut être exploitée par un individu mal intentionné afin d'exécuter du code arbitraire. Cette option n'est pas positionnée par défaut.

5 Solution

Mettre à jour Exim avec la version 4.32 et désactiver l'option `headers_check_syntax`.

6 Documentation

– Bulletin de sécurité #68 de Georgi Guninski :
http://www.guninski.com/exim1.html
– Bulletin de sécurité #DSA-501 de Debian :
http://www.debian.org/security/2004/dsa-501
– Bulletin de sécurité #DSA-502 de Debian :
http://www.debian.org/security/2004/dsa-502
– Bulletin de sécurité SUSE SuSE-SA:2004:012 du 14 mai 2004 :
http://www.suse.com/de/security/2004_12_mc.html
– Bulletin de sécurité Gentoo GLSA 200405-07 du 14 mai 2004 :
http://www.gentoo.org/security/en/glsa/glsa-200405-07.xml
– Référence CVE CAN-2004-0399 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0399
– Référence CVE CAN-2004-0400 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0400

Gestion détaillée du document

07 mai 2004 version initiale.
10 mai 2004 ajout de l'avis de sécurité Debian.
12 mai 2004 ajout des deux références CVE et ajout de l'avis de sécurité Debian relatif à exim-tls..
17 mai 2004 ajout des références aux bulletins de sécurité SUSE et Gentoo.