Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 3 septembre 2003
N° CERTA-2003-AVI-141-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de sendmail

Gestion du document

Référence	CERTA-2003-AVI-141-002
Titre	Vulnérabilité de sendmail
Date de la première version	27 août 2003
Date de la dernière version	3 septembre 2003
Source(s)	Avis 20030803-01-P de SGI Avis de sécurité SuSE-SA:2003:035 de SuSE Avis FreeBSD-SA-03:11 de FreeBSD Avis MDKSA-2003:086 de Mandrake
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

– Déni de service.

2 Systèmes affectés

Toutes les versions de sendmail 8.12.x.
La version 8.12.9 de sendmail corrige cette vulnérabilité.

3 Résumé

Une vulnérabilité présente dans le traitement de certaines requêtes DNS permet à un utilisateur mal intentionné de réaliser un déni de service par arrêt du serveur de messagerie sendmail.

4 Description

Sendmail, logiciel de routage de messages électroniques, peut collecter des informations sur des machines (fonctionnalité DNS MAPS) au moyen de requêtes DNS.

Une vulnérabilité de type débordement de mémoire présente dans le traitement de ces requêtes DNS permet à un utilisateur mal intentionné contrôlant un serveur DNS hostile de réaliser un déni de service par arrêt du serveur de messagerie sendmail.

Il est à noter que cette vulnérabilité n'est exploitable que si la primitive `FEATURE('enhdnsbl')` est présente dans le fichier de configuration de sendmail.

5 Solution

Installer sendmail 8.12.9 disponible sur le site sendmail.org :
http://www.sendmail.org/dnsmap1.html
ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité MDKSA-2003:086 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:086
- Bulletin de sécurité SuSE-SA:2003:035 de SuSE :
  http://www.suse.com/de/security/2003_035_sendmail.html
- Bulletin de sécurité 20030803-01-P de SGI :
  ftp://patches.sgi.com/support/free/security/advisories/20030803-01-P
- Bulletin de sécurité FreeBSD-SA-03:11 de FreeBSD :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:11.sendmail.asc
- Bulletin de sécurité RHSA-2003:265 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-265.html
- Bulletin de sécurité d'OpenBSD :
  http://www.openbsd.org/errata32.html#sendmail3

6 Documentation

- Référence CVE CAN-2003-0688 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0688
- Annonce "DNS map problem in 8.12.x before 8.12.9" :
  http://www.sendmail.org/dnsmap1.html
- Note VU#993452 du cert/cc :
  http://www.kb.cert.org/vuls/id/993452

Gestion détaillée du document

27 août 2003 version initiale.

29 août 2003 ajout référence au bulletin de sécurité de Red Hat.

3 septembre 2003 ajout référence au bulletin de sécurité d'OpenBSD.