

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le serveur de messagerie 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-2003-AVI-153>

Gestion du document

Référence	CERTA-2003-AVI-153-003
Titre	Vulnérabilités dans le serveur de messagerie Sendmail
Date de la première version	19 septembre 2003
Date de la dernière version	21 janvier 2004
Source(s)	Avis CA-2003-25 du CERT/CC
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 ;
- Exécution distante de code arbitraire avec les privilèges du service *sendmail* (généralement root).

2 Systèmes affectés

Tout système utilisant *Sendmail* dans une version antérieure à la 8.12.10, quel soit son type (*Unix/Linux, NT*).

3 Résumé

Deux failles ont été identifiées dans le code de *Sendmail* et l'une d'elle peut être exploitée à distance pour obtenir des privilèges élevés.

4 Description

Sendmail contient une vulnérabilité, de type débordement de tampon, dans le code d'analyse des adresses (référence CAN-2003-0694). Selon la plateforme et le système d'exploitation employé, celle-ci peut être utilisée pour exécuter du code localement et/ou à distance.

Par ailleurs, il existe également un bogue dans le code d'analyse des règles (référence CAN-2003-0681), non exploitable dans la configuration par défaut.

5 Solution

Mettre à jour *Sendmail*.

- Code source en version 8.12.10 au moins :
<http://www.sendmail.org/8.12.10.html>
- Linux Red Hat :
<https://rhn.redhat.com/errata/RHSA-2003-283.html>
- Mandrake Linux :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:092>
- Debian GNU/Linux :
<http://www.debian.org/security/2003/dsa-384>
- Slackware Linux :
<http://slackware.com/security/viewer.php?l=slackware-security&y=2003&m=slackware-security.452857>
- SuSE Linux :
http://www.suse.com/de/security/2003_040_sendmail.html
- Sun :
 - Solaris :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56860>
 - Linux et Cobalt :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56922>
- SGI Irix :
<ftp://patches.sgi.com/support/free/security/advisories/20030903-01-P.asc>
- HP-UX :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0309-281>
- IBM AIX :
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1473.1>
- FreeBSD :
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:13.sendmail.asc>
- OpenBSD :
<http://openbsd.org/errata.html#sendmail>

6 Documentation

- Référence CVE CAN-2003-0681 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0681>
- Référence CVE CAN-2003-0694 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0694>
- Avis du CERT/CC :
<http://www.cert.org/advisories/CA-2003-25.html>

Gestion détaillée du document

19 septembre 2003 version initiale ;

1er octobre 2003 ajout de SuSE, Sun, SGI, HP, IBM ;

20 janvier 2004 mise à jour pour IBM ;

21 janvier 2004 correction du lien IBM.