

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-034>

Gestion du document

Référence	CERTA-2003-AVI-034-003
Titre	Vulnérabilité de sendmail
Date de la première version	04 mars 2003
Date de la dernière version	14 mars 2003
Source(s)	Avis de sécurité ISS X-Force du 3 mars 2003
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 avec les privilèges de l'administrateur `root`.

2 Systèmes affectés

Toutes les versions de `sendmail` antérieures à la version 8.12.8.

3 Résumé

Une vulnérabilité dans la façon dont `sendmail` analyse les en-têtes des messages permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`Sendmail` est un logiciel de transport de mail (MTA : Mail Transport Agent). Une vulnérabilité a été découverte dans la façon dont `sendmail` analyse les en-têtes. Un utilisateur mal intentionné peut, via un message électronique habilement constitué, exécuter du code arbitraire à distance avec les privilèges de l'administrateur `root`.

5 Solution

La version 8.12.8 de sendmail corrige cette vulnérabilité.

6 Documentation

- Site internet de sendmail :
<http://www.sendmail.org>
- Avis de sécurité RedHat RHSA-2003:073-06 :
<https://rhn.redhat.com/errata/RHSA-2003-073.html>
- Avis de sécurité Mandrake MDKSA-2003:028 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:028>
- Avis de sécurité Suse SuSE-SA:2003:013 :
<http://www.suse.de/en/security>
- Avis de sécurité FreeBSD FreeBSD-SA-03:04.sendmail :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03%3A04.sendmail.asc>
- Avis de sécurité SGI IRIX #20030301-01-P :
<ftp://patches.sgi.com/support/free/security/advisories/20030301-01-P>
- Avis de sécurité HP Tru64 UNIX et HP-UX SSRT3469. Mise à jour à l'adresse suivante :
<ftp://ftp.itrc.hp.com/>
- Mise à jour de sendmail sous IBM AIX :
<ftp://aix.software.ibm.com/aix/efixes/security/>
- Avis de sécurité Debian DSA-257-1 :
<http://www.debian.org/security/>
- Avis de sécurité Apple APPLE-SA-2003-03-03 sendmail :
http://www.apple.com/support/security/security_updates.html
- Avis de sécurité Gentoo GLSA sendmail (200303-4) :
<http://www.gentoo.org>
- Avis de sécurité OpenBSD 009 :
<http://www.openbsd.org/errata.html#sendmail>
- Avis de sécurité NetBSD SA2003-002 :
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-002.txt.asc>
- Avis de sécurité UnixWare CSSA-2003-SCO.5 :
<ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.5/CSSA-2003-SCO.5.txt>
- Avis de sécurité OpenServer CSSA-2003-SCO.6 :
<ftp://ftp.sco.com/pub/updates/OpenServer/CSSA-2003-SCO.6/CSSA-2003-SCO.6.txt>

Gestion détaillée du document

04 mars 2003 version initiale.

04 mars 2003 ajout du bulletin de sécurité Debian, Apple et Gentoo.

10 mars 2003 ajout des bulletins de sécurité OpenBSD, NetBSD et UnixWare.

14 mars 2003 ajout du bulletin de sécurité OpenServer.