

Affaire suivie par :
CERTA

BULLETIN D'ALERTE 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-2006-ALE-003>

Gestion du document

Référence	CERTA-2006-ALE-003
Titre	Vulnérabilité de Sendmail
Date de la première version	24 mars 2006
Date de la dernière version	-
Source(s)	Bulletin de sécurité du CERTA CERTA-2006-AVI-124 du 23 mars 2006
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 ;
- déni de service à distance.

2 Systèmes affectés

- Pour la branche 8.12.x, Sendmail version 8.12.11 et versions antérieures ;
- pour la branche 8.13.x, Sendmail version 8.13.5 et versions antérieures.

3 Résumé

Une vulnérabilité dans le logiciel de messagerie Sendmail permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance. Le fort déploiement de Sendmail combiné à la gravité de la faille a conduit le CERTA à augmenter le niveau de vigilance au niveau d'alerte, en plus de l'avis CERTA-2006-AVI-124 publié la jeudi 23 mars 2006.

L'objectif de cette alerte est de sensibiliser les utilisateurs à la nécessité d'appliquer les correctifs en fonction des systèmes concernés.

4 Description

Sendmail est un logiciel de routage de messages électroniques (Mail Transport Agent ou MTA). Une vulnérabilité dans la gestion de messages asynchrones par le logiciel Sendmail permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance sur la machine vulnérable.

5 Solution

Mettre à jour Sendmail en version 8.13.6. En plus de ce problème de sécurité, Sendmail version 8.13.6 corrige d'autres problèmes de sécurité et d'autres faiblesses dans le code. Sendmail 8.13.6 peut se télécharger à l'adresse suivante :

<http://www.sendmail.org/8.13.6.html> Si la mise à jour de Sendmail en version 8.13.6 n'est pas possible, appliquer les correctifs pour Sendmail 8.12.11 et 8.13.5. Les correctifs sont disponibles aux adresses suivantes :

<ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0>

<ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0> Dans tous les cas, se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de Sendmail :
<http://www.sendmail.com>
- Page Internet de la version 8.13.6 de Sendmail :
<http://www.sendmail.org/8.13.6.html>
- Bulletin de sécurité Sendmail du 22 mars 2006 :
<http://www.sendmail.com/company/advisory/index.shtml>
- Bulletin de sécurité CERTA-2006-AVI-124 du jeudi 23 mars 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-124/index.html>
- Alerte de sécurité de l'US-CERT TA06-081A et VU#834865 du 22 mars 2006 :
<http://www.us-cert.gov/cas/techalerts/TA06-081A.html>
<http://www.kb.cert.org/vuls/id/834865>
- Bulletin de sécurité ISS du 22 mars 2006 :
<http://xforce.iss.net/xforce/alerts/id/216>
- Bulletin de sécurité Gentoo GLSA-200603-21 du 22 mars 2006 :
<http://www.gentoo.org/security/en/glsa/glsa-200603-21.xml>
- Bulletin de sécurité Mandriva MDKSA-2006:058 du 22 mars 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:058>
- Bulletin de sécurité RedHat RHSA-2006:0264 du 22 mars 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0264.html>
- Bulletin de sécurité RedHat RHSA-2006:0265 du 22 mars 2006 :
<http://rhn.redhat.com/errata/RHSA-2006-0265.html>
- Bulletin de sécurité SUSE SuSE-SA:2006:017 du 22 mars 2006 :
http://www.novell.com/linux/security/advisories/2006_17_sendmail.html
- Bulletin de sécurité FreeBSD SA-06:13.sendmail du 22 mars 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:13.sendmail.asc>
- Mises à jour de sécurité pour Fedora du 22 mars 2006 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/>
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/5/>
- Bulletin de sécurité Slackware SSA:2006-081-01 du 22 mars 2003 :
<http://slackware.com/security/viewer.php?l=slackware-security&y=2006&m=slackware-security.619600>
- Bulletin de sécurité Sun Alerte #102262 du 22 mars 2006 :
<http://sunsolve.sun.com/search/document.do?assetKey=1-26-102262-1>
- Bulletin de sécurité Debian DSA-1015 du 23 mars 2006 :
<http://www.debian.org/security/2006/dsa-1015>

- Bulletin de sécurité IBM AIX du 23 mars 2006 :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY82992>
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY82993>
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY82994>
- Référence CVE CVE-2006-0058 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0058>

Gestion détaillée du document

24 mars 2006 version initiale.