

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Emacs et XEmacs

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-2005-AVI-067>

Gestion du document

Référence	CERTA-2005-AVI-067-005
Titre	Vulnérabilité de Emacs et XEmacs
Date de la première version	11 février 2005
Date de la dernière version	24 février 2005
Source(s)	Bulletins de sécurité Debian DSA-670 et DSA-671
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.

2 Systèmes affectés

- Emacs versions 20.x ;
- Emacs version 21.3 et versions antérieures ;
- XEmacs version 21.4 et versions antérieures.

3 Description

Une vulnérabilité dans l'utilitaire `movemail` de Emacs et XEmacs permet à un utilisateur mal intentionné, via un serveur POP3 malicieusement constitué, d'exécuter du code arbitraire avec les droits de l'application Emacs ou XEmacs.

4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet de Emacs :
<http://www.gnu.org/software/emacs/emacs.html>
- Site Internet de XEmacs :
<http://www.xemacs.org>
- Bulletin de sécurité Debian DSA-670 du 08 février 2005 :
<http://www.debian.org/security/2005/dsa-670>
- Bulletin de sécurité Debian DSA-671 du 08 février 2005 :
<http://www.debian.org/security/2005/dsa-671>
- Bulletin de sécurité Debian DSA-685 du 17 février 2005 :
<http://www.debian.org/security/2005/dsa-685>
- Bulletin de sécurité Gentoo GLSA 200502-20 du 15 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-20.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:038 du 15 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:038>
- Bulletin de sécurité RedHat RHSA-2005:112 du 10 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-112.html>
- Bulletin de sécurité RedHat RHSA-2005:134 du 10 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-134.html>
- Bulletin de sécurité RedHat RHSA-2005:110 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-110.html>
- Bulletin de sécurité RedHat RHSA-2005:133 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-133.html>
- Bulletin de sécurité OpenBSD pour emacs et Xemacs du 09 février 2005 :
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité FreeBSD pour emacs et xemacs du 14 février 2005 :
<http://www.vuxml.org/freebsd/>
- Mises à jour de sécurité des paquetages NetBSD emacs, emacs-nox11, emacs20, xemacs, xemacs-nox11 et xemacs-current :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/emacs/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/emacs-nox11/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/emacs20/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/xemacs/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/xemacs-nox11/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/editors/xemacs-current/README.html>
- Référence CVE CAN-2005-0100 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0100>

Gestion détaillée du document

11 février 2005 version initiale.

14 février 2005 ajout de la référence au bulletin de sécurité FreeBSD.

16 février 2005 ajout de la référence aux bulletins de sécurité Gentoo et Mandrake.

17 février 2005 ajout de la référence aux bulletins de sécurité RedHat RHSA-2005:110 et RHSA-2005:133.

18 février 2005 ajout de la référence au bulletin de sécurité Debian DSA-685.

24 février 2005 ajout des références aux bulletins de sécurité NetBSD.