



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2005
N° CERTA-2005-AVI-278-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Fetchmail

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-278>

Gestion du document

Référence	CERTA-2005-AVI-278-005
Titre	Vulnérabilité dans Fetchmail
Date de la première version	22 juillet 2005
Date de la dernière version	17 août 2005
Source(s)	Bulletin de sécurité Berlios
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 via un serveur POP3 malicieux ;
- déni de service.

2 Systèmes affectés

Fetchmail version 6.2.5.1 et versions antérieures.

3 Description

cette vulnérabilité et injecter du code arbitraire à distance permettant, entre autres, d'obtenir les droits administrateurs sur la machine vulnérable.

L'exploitation de cette faille à destination d'une machine disposant de Fetchmail 6.2.5.1 ne provoque qu'un déni de service.

4 Solution

Passer en version 6.2.5.2 et appliquer le patch fetchmail-patch-6.2.5.2 :
http://developer.berlios.de/project/showfiles.php?group_id=1824

5 Documentation

- Bulletin de sécurité Berlios :
<http://fetchmail.berlios.de/fetchmail-SA-2005-01.txt>
- Bulletin de sécurité de FreeBSD :
<http://www.vuxml.org/freebsd/pkg-fetchmail.html>
- Bulletin de sécurité RedHat RHSA-2005:640 du 25 juillet 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-640.html>
- Bulletin de sécurité OpenBSD pour fetchmail du 25 juillet 2005 :
<http://www.vuxml.org/openbsd/pkg-fetchmail.html>
- Bulletin de sécurité Debian DSA-774 du 12 août 2005 :
<http://www.debian.org/security/2005/dsa-774>
- Bulletin de sécurité Gentoo GLSA 200507-21 du 25 juillet 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200507-21.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:126 du 28 juillet 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:126>
- Bulletin de sécurité SUSE SUSE-SR:2005:018 du 28 juillet 2005 :
http://www.novell.com/linux/security/advisories/2005_18_sr.html
- Référence CVE CAN-2005-2335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2335>

Gestion détaillée du document

22 juillet 2005 version initiale.

25 juillet 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:640 et de la référence CVE CAN-2005-2335.

25 juillet 2005 ajout de la référence au bulletin de sécurité OpenBSD.

26 juillet 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200507-21.

29 juillet 2005 ajout des références aux bulletins de sécurité Mandriva MDKSA-2005:126 et SUSE SUSE-SR:2005:018.

17 août 2005 ajout de la référence au bulletin de sécurité Debian DSA-774.