

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Exim

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-014>

Gestion du document

Référence	CERTA-2005-AVI-014-003
Titre	Multiples vulnérabilités dans Exim
Date de la première version	13 janvier 2005
Date de la dernière version	17 février 2005
Source(s)	Bulletin de sécurité d'iDEFENSE Bulletin de sécurité d'Exim
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire ;
- élévation de privilèges.

2 Systèmes affectés

Versions antérieures à Exim 4.44.

3 Résumé

Trois vulnérabilités présentes dans l'application Exim permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance et d'élever ses privilèges.

4 Description

Exim est un logiciel de service de messagerie sous Unix.

L'application Exim présente une vulnérabilité de type dépassement de mémoire tampon dans la fonction `host_aton()`. Cette vulnérabilité permet à une personne malveillante d'exécuter du code arbitraire au moyen d'une adresse IPv6 malicieusement constituée.

Une seconde vulnérabilité découverte dans la fonction `spa_base64_to_bits()` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance, due à une faiblesse lors de l'authentification SPA (Secure Password Authentication basée sur Windows NTLM).

La dernière vulnérabilité de type dépassement de la mémoire tampon permet à un utilisateur mal intentionné d'exécuter du code arbitraire. Une personne malveillante peut exploiter la vulnérabilité présente dans `dns_build_reverse()` au moyen d'un paramètre malicieusement construit, fournit en argument à la fonction.

Exim est le serveur de messagerie par défaut des distributions Debian GNU/Linux.

5 Solution

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

6 Documentation

- Site Internet d'Exim :
<http://www.exim.org>
- Bulletin de sécurité d'IDEFENSE "Exim `auth_spa_server()` Buffer Overflow" du 07 janvier 2005 :
<http://www.odefense.com/application/poi/display?id=178&type=vulnerabilities>
- Bulletin de sécurité d'IDEFENSE "Exim `host_aton()` Buffer Overflow" du 07 janvier 2005 :
<http://www.odefense.com/application/poi/display?id=179&type=vulnerabilities>
- Bulletin de sécurité Debian DSA-635 du 12 janvier 2005 :
<http://www.debian.org/security/2005/dsa-635>
- Bulletin de sécurité Debian DSA-637 du 13 janvier 2005 :
<http://www.debian.org/security/2005/dsa-637>
- Bulletin de sécurité Gentoo GLSA-200501-23 du 12 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-23.xml>
- Bulletin de sécurité RedHat RHSA-2005:025 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-025.html>
- Bulletin de sécurité FreeBSD pour CVS du 05 janvier 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité OpenBSD pour CVS du 26 janvier 2004 :
<http://www.vuxml.org/openbsd/>
- Mise à jour de sécurité du paquetage NetBSD `cvs` :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/exim/README.html>
- Référence CVE CAN-2005-0021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0021>
- Référence CVE CAN-2005-0022 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0022>
- Note de vulnérabilité #132992 de l'US-CERT du 27 janvier 2005 :
<http://www.kb.cert.org/vuls/id/132992>

Gestion détaillée du document

13 janvier 2005 version initiale ;

21 janvier 2005 ajout d'une nouvelle vulnérabilité découverte dans Exim ;

1er février 2005 ajout des références à un second bulletin Debian, aux bulletins de sécurité OpenBSD, FreeBSD et NetBSD, et de la note de vulnérabilité de l'US-CERT.

17 février 2005 ajout référence au bulletin de sécurité RedHat RHSA-2005-025.