

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de rsync

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-2004-AVI-271>

Gestion du document

Référence	CERTA-2004-AVI-271-003
Titre	Vulnérabilité de rsync
Date de la première version	17 août 2004
Date de la dernière version	02 septembre 2004
Source(s)	Avis de sécurité rsync
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

rsync versions 2.6.2 et antérieures.

3 Résumé

Une vulnérabilité de *rsync* permet à un utilisateur mal intentionné d'accéder à n'importe quel fichier de la machine.

4 Description

rsync est un utilitaire utilisé pour la copie de fichiers.

Une vulnérabilité a été découverte dans *rsync*, et permet à un utilisateur mal intentionné d'accéder à des fichiers situés en dehors du répertoire de base.

Pour exploiter cette vulnérabilité, il faut que *rsync* soit lancé en *modedémon* et sans "*chroot*".

5 Contournement provisoire

- Ne pas lancer *rsync* en *modedémon* ;
- utiliser un "*chroot*".

6 Solution

La version 2.6.3pre1 corrige cette vulnérabilité. Se référer au bulletin de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site Internet de *rsync* :
<http://samba.org/rsync/>
- Avis de sécurité *rsync* d'août 2004 :
http://samba.org/rsync/#security_aug04
- Bulletin de sécurité Debian DSA-538 du 17 août 2004 :
<http://www.debian.org/security/2004/dsa-538>
- Bulletin de sécurité Gentoo GLSA-200408-17 du 17 août 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200408-17.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:083 du 17 août 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:083>
- Bulletin de sécurité SUSE SuSE-SA:2004:026 du 16 août 2004 :
http://www.suse.com/de/security/2004_26_rsync.html
- Bulletin de sécurité RedHat RHSA-2004:436 du 01 septembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-436.html>
- Bulletin de sécurité OpenBSD pour *rsync* du 14 août 2004 :
<http://www.vuxml.org/openbsd>
- Bulletin de sécurité FreeBSD pour *rsync* du 26 août 2004 :
<http://www.vuxml.org/freebsd>
- Mise à jour de sécurité du paquetage NetBSD *rsync* :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/rsync/README.html>
- Référence CVE CAN-2004-0792 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0792>

Gestion détaillée du document

17 août 2004 version initiale.

19 août 2004 ajout des références aux bulletins de sécurité Gentoo et Mandrake, et ajout référence CVE.

30 août 2004 ajout des références aux bulletins de sécurité FreeBSD et NetBSD.

02 septembre 2004 ajout de la référence au bulletin de sécurité RedHat.