

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-2003-AVI-206>

Gestion du document

Référence	CERTA-2003-AVI-206-003
Titre	Vulnérabilité de rsync
Date de la première version	4 décembre 2003
Date de la dernière version	10 mars 2004
Source(s)	Bulletin de sécurité rsync du 4 décembre 2003
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.

2 Systèmes affectés

Rsync 2.5.6 et versions antérieures.

3 Description

rsync est un utilitaire qui permet de synchroniser des fichiers entre plusieurs machines.

Une vulnérabilité de type débordement de mémoire présente dans rsync en mode serveur peut être exploitée à distance par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur le serveur vulnérable.

4 Contournement provisoire

Pour se protéger contre une attaque venant de l'extérieur, il est recommandé de filtrer le port 873/tcp sur les pare-feux.

5 Solution

Installer la version 2.5.7 de `rsync`.

6 Documentation

- Site de `rsync` :
<http://rsync.samba.org>
- Bulletin de sécurité DSA-404 de Debian :
<http://www.debian.org/security/2003/dsa-404>
- Bulletin de sécurité MDKSA-2003:111 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:111>
- Bulletin de sécurité SuSE-SA:2003:50 de SuSE :
http://www.suse.com/de/security/2003_50_rsync.html
- Bulletin de sécurité RHSA-2003:388 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-388.html>
- Bulletin de sécurité GLSA 200312-03 de Gentoo :
<http://www.securityfocus.com/advisories/6142>
- Correctifs de sécurité de Sun pour les produits Sun Cobalt Qube 3, RaQ 4 et RaQ 550 :
<http://ftp.cobalt.sun.com/pub/packages/>
- Correctifs de sécurité de Sun pour les produits Sun Cobalt RaQ XTR :
<http://ftp.cobalt.sun.com/pub/packages/raqxtr/eng/RaQXTR-All-Security-1.0.1-16675.pkg>
- Référence CVE CAN-2003-0962 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0962>

Gestion détaillée du document

4 décembre 2003 version initiale.

5 décembre 2003 Ajout référence CVE et références aux bulletins de sécurité de Mandrake, Debian, SuSE, Red Hat et Gentoo.

17 février 2004 Ajout de la référence aux correctifs de sécurité de Sun pour les Sun Cobalt Qube3, RaQ 4 et RaQ 550.

10 mars 2004 Ajout de la référence au correctif de Sun pour Sun Cobalt RaQ XTR.