



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 octobre 2004
N° CERTA-2004-AVI-332-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Samba

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-332>

Gestion du document

Référence	CERTA-2004-AVI-332-002
Titre	Vulnérabilité de Samba
Date de la première version	08 octobre 2004
Date de la dernière version	22 octobre 2004
Source(s)	Bulletin de sécurité Samba 2.2.12 du 29 septembre 2004
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

- Samba 2.2.12 et versions antérieures ;
- Samba 3.0.5 et versions antérieures.

3 Résumé

Une vulnérabilité dans Samba permet à un utilisateur mal intentionné d'avoir accès de manière arbitraire aux informations présentes sur le système.

4 Description

Samba est un logiciel libre, open source, utilisé pour la mise en œuvre des partages réseau à l'aide des protocoles SMB et CIFS sous Unix.

Une vulnérabilité présente lors de l'appel des fonctions `unix_convert()` et `check_name()` permet à une personne malveillante d'avoir accès à des informations hors du répertoire partagé.

5 Solution

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

6 Documentation

- Site de l'éditeur Samba :
<http://www.samba.org>
- Note "Samba 2.2.12 Potential Arbitrary File Access" :
<http://sambafr.idealx.org/samba/history/samba-2.2.12.html>
- Bulletin de sécurité "Samba Arbitrary File Access Vulnerability" d'IDEFENSE :
<http://www.odefense.com/application/poi/display?id=146&type=vulnerabilities>
- Bulletin de sécurité Debian DSA-600 du 07 octobre 2004 :
<http://www.debian.org/security/2004/dsa-600>
- Bulletin de sécurité de SUSE SuSE-SA:2004:035 du 05 octobre 2004 :
http://www.suse.com/de/security/2004_35_samba.html
- Bulletin de sécurité RedHat Enterprise Linux et RedHat Desktop :
<http://rhn.redhat.com/errata/RHSA-2004-498.html>
- Bulletin de sécurité RedHat et Fedora produits "End-of-Life" :
http://www.fedoralegacy.org/updates/RH9/2004-10-13-FLSA_2004_2102__Updated_samba_packages_fix_security_vulnerab
- Bulletin de sécurité de FreeBSD pour Samba du 30 septembre 2004:
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité HP (HPSBUX01086) :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01086>
- Référence CVE CAN-2004-0815 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0815>

Gestion détaillée du document

08 octobre 2004 version initiale.

14 octobre 2004 ajout référence au bulletin de sécurité RedHat (RHSA-2004-498) et au bulletin de sécurité de Fedora (FLSA:2102).

22 octobre 2004 ajout référence au bulletin de sécurité HP (HPSBUX01086).