



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 février 2005
N° CERTA-2004-AVI-402-007

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-402>

Gestion du document

Référence	CERTA-2004-AVI-402-007
Titre	Vulnérabilité de Samba
Date de la première version	17 décembre 2004
Date de la dernière version	04 février 2005
Source(s)	Bulletin de sécurité d'iDEFENSE Bulletin de sécurité de Samba
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

Elévation de privilèges.

2 Systèmes affectés

Samba 3.0.9 et versions antérieures.

3 Description

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

Une vulnérabilité de type débordement de mémoire est présente dans le processus `smbd` lors du traitement des paramètres de sécurité associés à un fichier. Un utilisateur distant, préalablement authentifié, peut utiliser cette vulnérabilité pour exécuter du code arbitraire à distance avec les privilèges du super-utilisateur `root` sur le système vulnérable.

4 Solution

La version 3.0.10 de Samba corrige cette vulnérabilité.

5 Documentation

- Bulletin de sécurité de samba :
<http://us1.samba.org/samba/security/CAN-2004-1154.html>
- Bulletin de sécurité d'iDEFENSE "Samba smbdc security descriptor integer overflow vulnerability" du 16 décembre 2004 :
<http://www.idefense.com/application/poi/display?id=165&type=vulnerabilities>
- Bulletin de sécurité Red Hat RHSA-2004-670 du 16 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-670.html>
- Bulletin de sécurité Red Hat RHSA-2005-020 du 05 janvier 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-020.html>
- Bulletin de sécurité Red Hat RHSA-2004-681 du 21 décembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-681.html>
- Bulletin de sécurité Gentoo GLSA-200412-13 du 17 décembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200412-13.xml>
- Bulletin de sécurité SuSE SUSE-SA:2004:045 du 22 décembre 2004 ;
http://www.novell.com/linux/security/advisories/2004_45_samba.html
- Bulletin de sécurité FreeBSD du 21 décembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité Mandrake MDKSA-2004:158 du 27 décembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:158>
- Bulletin de sécurité HP HPSBUX01115 du 02 février 2005 :
<http://itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01115>
- Bulletin de sécurité Sun #57730 du 03 février 2005 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-57730-1>
- Référence CVE CAN-2004-1154 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1154>

Gestion détaillée du document

17 décembre 2004 version initiale.

20 décembre 2004 ajout référence aux bulletins de sécurité de Red Hat et Gentoo.

21 décembre 2004 ajout référence au bulletin de sécurité de FreeBSD.

22 décembre 2004 ajout référence au bulletin de sécurité Red Hat RHSA-2004-681.

23 décembre 2004 ajout référence au bulletin de sécurité SuSE SUSE-SA:2004:045.

03 janvier 2005 ajout référence au bulletin de sécurité Mandrake MDKSA-2004:158.

06 janvier 2005 ajout référence au bulletin de sécurité Red Hat RHSA-2005-020.

04 février 2005 ajout références aux bulletins de sécurité HP HPSBUX01115 et Sun #57730.