

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-368>

Gestion du document

Référence	CERTA-2004-AVI-368-003
Titre	Multiples vulnérabilités de Samba
Date de la première version	17 novembre 2004
Date de la dernière version	16 décembre 2004
Source(s)	Bulletin de sécurité d'iDEFENSE Bulletin de sécurité d'e-matters
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

Samba 3.0.7 et versions antérieures.

3 Résumé

Samba 3.0.8 corrige deux vulnérabilités présentes dans les versions antérieures de Samba.

4 Description

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

Deux vulnérabilités sont présentes dans Samba :

- CVE CAN-2004-882 : une vulnérabilité de type débordement de mémoire est présente dans le traitement des requêtes QFILEPATHINFO. En créant au préalable sur un serveur Samba des fichiers dont le nom est soigneusement choisi, un utilisateur mal intentionné peut réaliser l'exécution de code arbitraire à distance sur un serveur Samba vulnérable.
- CVE CAN-2004-930 : une vulnérabilité est présente dans le traitement des noms de fichiers contenant le caractère '*'. Par le biais de requêtes habilement constituées, un utilisateur mal intentionné peut réaliser un déni de service par consommation excessive de ressources processeur.

5 Solution

La version 3.0.8 de Samba corrige ces vulnérabilités.

6 Documentation

- Site de Samba :
<http://www.samba.org>
- Bulletin de sécurité d'e-matters "Samba 3.x QFILEPATHINFO unicode filename buffer overflow" du 15 novembre 2004 :
<http://security.e-matters.de/advisories/132004.html>
- Bulletin de sécurité d'iDEFENSE "Samba SMBD remote denial of service vulnerability" du 08 novembre 2004 :
<http://www.idefense.com/application/poi/display?id=156&type=vulnerabilities>
- Annonce Samba "CAN-2004-0930: Potential remote denial of service vulnerability in Samba 3.0.x <= 3.0.7" :
<http://sambafr.idealx.org/samba/security/CAN-2004-0930.html>
- Bulletin de sécurité Mandrake MDKSA-2004:131 du 10 novembre 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:131>
- Bulletin de sécurité Mandrake MDKSA-2004:136 du 18 novembre 2004 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:136>
- Bulletin de sécurité Gentoo GLSA 200411621 du 15 novembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200411-21.xml>
- Bulletin de sécurité SuSE SuSE-SA:2004:40 du 15 novembre 2004 :
http://www.suse.com/de/security/2004_40_samba.html
- Bulletin de sécurité Red Hat RHSA-2004:632 du 16 novembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-632.html>
- Bulletin de sécurité de FreeBSD pour Samba du 12 novembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité de FreeBSD pour smbd du 17 novembre 2004 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité SGI (IRIX) 20041201-01-P du 07 décembre 2004 :
<ftp://patches.sgi.com/support/free/security/advisories/20041201-01-P.asc>
- Référence CVE CAN-2004-0882 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0882>
- Référence CVE CAN-2004-0930 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0930>

Gestion détaillée du document

17 novembre 2004 version initiale.

19 novembre 2004 ajout de la référence au bulletin de sécurité MDKSA-2004:136 de Mandrake.

22 novembre 2004 ajout de la référence au second bulletin de sécurité FreeBSD.

16 décembre 2004 ajout de la référence au bulletin de sécurité SGI.