Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 juillet 2004
N° CERTA-2004-AVI-251-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Samba

Gestion du document

Référence	CERTA-2004-AVI-251-005
Titre	Vulnérabilité de Samba
Date de la première version	23 juillet 2004
Date de la dernière version	30 juillet 2004
Source(s)	Bulletin de sécurité RedHat RHSA-2004:259
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Samba version 2.2.0 jusqu'à la version 2.2.9 ;
- Samba version 3.0.0 jusqu'à la version 3.0.4.

3 Résumé

Plusieurs vulnérabilités de Samba permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

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

Deux vulnérabilités ont été découvertes :

- Une première vulnérabilité concerne un débordement de mémoire dans l'outil de gestion Samba accessible à travers un navigateur, nommé `SWAT` (`Samba Web Administration Tool`). Ce débordement de mémoire intervient dans le décodage `base64` lors d'une authentification basique (`basic authentication`) ainsi que lors du décodage de l'attribut `sambaMungeDial` lors de l'utilisation de `ldapsam passdb` (CVE CAN-2004-0600).
  Cette première vulnérabilité affecte seulement la branche Samba 3.0.x.
- une seconde vulnérabilité concerne un débordement de mémoire dans le code gérant l'option `mangling method = hash` du fichier de configuration `smb.conf` (CVE CAN-2004-0686).
  Cette seconde vulnérabilité affecte les branches Samba 2.2.x et 3.0.x.

5 Contournement provisoire

- Concernant la vulnérabilité CVE CAN-2004-0600, désactiver le service d'administration `SWAT` et vérifier les droits d'accès en écriture aux attributs `sambaSamAccount`.
- concernant la vulnérabilité CVE CAN-2004-0686, ne pas spécifier l'option `mangling method = hash` dans le fichier de configuration `smb.conf`. Utiliser `mangling method = hash2` à la place (normalement il s'agit de la valeur par défaut).

6 Solution

- A partir des sources, mettre à jour Samba en version 2.2.10 ou en version 3.0.5.
  Les sources de Samba sont téléchargeables à l'adresse suivante :
  http://download.samba.org/samba/ftp/
- Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site Internet de Samba :
  http://www.samba.org
- Note relative à la sortie de Samba 2.2.10 :
  http://www.samba.org/samba/whatsnew/samba-2.2.10.html
- Note relative à la sortie de Samba 3.0.5 :
  http://www.samba.org/samba/whatsnew/samba-3.0.5.html
- Bulletin de sécurité RedHat RHSA-2004:259 du 22 juillet 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-259.html
- Bulletin de sécurité RedHat RHSA-2004:404 du 26 juillet 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-404.html
- Bulletin de sécurité Mandrake MDKSA-2004:071 du 22 juillet 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:071
- Bulletin de sécurité SUSE SUSE-SA:2004:022 du 23 juillet 2004 :
  http://www.suse.com/de/security/2004_22_samba.html
- Bulletin de sécurité Gentoo GLSA 200407-21 du 29 juillet 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200407-21.xml
- Bulletin de sécurité FreeBSD pour samba du 21 juillet 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité OpenBSD pour samba du 23 juillet 2004 :
  http://www.vuxml.org/openbsd/
- Mise à jour de sécurité des paquetages NetBSD samba et ja-samba :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/samba/README.html
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/ja-samba/README.html
- Bulletin de sécurité HP HPSBUX01062 "HP-UX CIFS server potential remote root access" du 26 juillet 2004 :
  http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01062

- Référence CVE CAN-2004-0600 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0600
- Référence CVE CAN-2004-0686 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0686

Gestion détaillée du document

23 juillet 2004 version initiale.
23 juillet 2004 ajout de la référence au bulletin de sécurité SUSE.
26 juillet 2004 ajout des références aux bulletins de sécurité OpenBSD et NetBSD.
27 juillet 2004 ajout de la référence au bulletin de sécurité RHSA-2004:404 de RedHat.
28 juillet 2004 ajout de la référence au bulletin de sécurité HP-UX.
30 juillet 2004 ajout de la référence au bulletin de sécurité Gentoo.