

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-2007-AVI-068>

Gestion du document

Référence	CERTA-2007-AVI-068-001
Titre	Multiples vulnérabilités de Samba
Date de la première version	06 février 2007
Date de la dernière version	10 avril 2007
Source(s)	Bulletin de sécurité Debian DSA-1257
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 à distance.

2 Systèmes affectés

Samba 3.0.23d et versions antérieurs.

3 Résumé

Trois vulnérabilités de *Samba* permettent de provoquer un déni de service à distance et l'exécution de code arbitraire à distance.

4 Description

Le logiciel *Samba* est un logiciel libre de partage de ressources qui utilise le protocole SMB (*Server Message Block*).

Un défaut de validation des entrées de l'utilisateur permettrait à une personne malveillante d'exécuter à distance un code arbitraire, dans le contexte de l'utilisateur.

Un défaut de validation d'entrée dans les fonctions `gethostbyname()` et `getipnodebyname()` permettrait l'exécution de code arbitraire à distance lorsque le service `winbind` est activé.

Une erreur dans `smbd` permettrait à un utilisateur authentifié de provoquer une boucle infinie et ainsi un déni de service à distance.

5 Solution

La version 3.0.24 de *Samba* corrige le problème. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site du projet Samba :
<http://www.samba.org/>
- Bulletin de sécurité Debian DSA 1257 du 05 février 2007 :
<http://www.debian.org/security/2007/dsa-1257>
- Référence CVE CVE-2007-0452 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0452>
- Référence CVE CVE-2007-0453 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0453>
- Référence CVE CVE-2007-0454 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0454>
- Bulletin de sécurité SUSE SA:2007-016 du 15 février 2007 :
<http://lists.suse.com/archive/suse-security-announce/2007-Feb/0002.html>
- Bulletin de sécurité Red Hat (CVE-2007-0452) RHSA-2007-0061-2 du 14 mars 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0061.html>
- Bulletin de sécurité Red Hat (CVE-2007-0452) RHSA-2007-0060-3 du 15 février 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0060.html>
- Bulletin de sécurité Mandriva MDKSA-2007-034 du 5 février 2007 (CVE-2007-0452, CVE-2007-0454) :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:034>
- Bulletin de sécurité Gentoo GLSA 200702-01 du 13 février 2007 (CVE-2007-0452, CVE-2007-0454) :
<http://www.gentoo.org/security/en/glsa/glsa-200702-01.xml>
- Bulletin de sécurité Ubuntu USN-419-1 du 6 février 2007 (CVE-2007-0452, CVE-2007-0454) :
<http://www.ubuntu.com/usn/usn-419-1>
- Bulletin de sécurité HP-UX du 04 avril 2007 (CVE-2007-0452) :
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c00943462>

Gestion détaillée du document

06 février 2007 version initiale.

10 avril 2007 ajout des références aux bulletins de sécurité de Ubuntu, Mandriva, HP-UX, Gentoo, et SuSE.