

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-502>

Gestion du document

Référence	CERTA-2007-AVI-502-002
Titre	Vulnérabilités dans Samba
Date de la première version	16 novembre 2007
Date de la dernière version	13 mars 2008
Source(s)	Bulletin de sécurité de Samba du 15 novembre 2007
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.

2 Systèmes affectés

Samba, versions 3.0.x.

3 Description

Une vulnérabilité dans la construction de réponses d'un serveur Samba à des requêtes Netbios permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

Une autre vulnérabilité, exploitable uniquement si le serveur Samba sert de contrôleur de domaine primaire ou secondaire, permet également à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Fedora 3402 du 15 novembre 2007 :
<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00472.html>
- Bulletin de sécurité RedHat RHSA-2007:1013 du 15 novembre 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-1013.html>
- Bulletin du projet Samba du 15 novembre 2007 :
<http://us1.samba.org/samba/history/security.html>
- Bulletin de sécurité Ubuntu USN-544-1 du 15 novembre 2007 :
<http://www.ubuntulinux.org/usn/usn-544-1>
- Bulletin de sécurité Gentoo GLSA 200711-29 du 20 novembre 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200711-29.xml>
- Bulletin de sécurité Mandriva MDKSA-2007:224-1 du 21 novembre 2007 :
<http://www.mandriva.com/en/security/advisories?name=MDKSA-2007:224-1>
- Bulletin de sécurité Debian DSA-1409 du 29 novembre 2007 :
<http://www.debian.org/security/2007/dsa-1409>
- Référence CVE CVE-2007-4572 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4572>
- Référence CVE CVE-2007-5398 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5398>
- Référence CVE CVE-2007-6015 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6015>
- Bulletin de sécurité HP-UX HPSBUX02316 du 10 mars 2008 :
<http://itrc.hp.com/service/cki/docDisplay.do?docId=c01377687>

Gestion détaillée du document

16 novembre 2007 version initiale.

30 novembre 2007 ajout des références aux bulletins de sécurité Mandriva, Gentoo et Debian.

13 mars 2008 ajout de la référence au bulletin de sécurité HP-UX.