



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2010
N° CERTA-2010-AVI-266-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2010-AVI-266>

Gestion du document

Référence	CERTA-2010-AVI-266-001
Titre	Vulnérabilité dans Samba
Date de la première version	16 juin 2010
Date de la dernière version	29 novembre 2010
Source(s)	Bulletin de sécurité du projet Samba du 16 juin 2010
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.x à 3.3.12.
Les versions 3.4.0 et suivantes de Samba ne sont pas concernées.

3 Résumé

Une erreur de traitement de SMB1 par le serveur Samba permet à un utilisateur malveillant de provoquer un déni de service à distance et permettrait d'exécuter du code arbitraire à distance.

4 Description

Une erreur est présente dans le traitement du chaînage des paquets SMB1 par le serveur Samba. Un défaut de validation des données de l'utilisateur provoque une corruption de la mémoire. Cette vulnérabilité permet à

un utilisateur malveillant non authentifié de provoquer un déni de service à distance, voire d'exécuter du code arbitraire à distance.

5 Solution

La version 3.3.13 de Samba remédie à ce problème.

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

6 Documentation

- Bulletin de sécurité du projet Samba du 16 juin 2010 :
<http://www.samba.org/samba/security/CVE-2010-2063.html>
- Bulletin de sécurité Apple HT4312 du 07 octobre 2010 :
<http://support.apple.com/kb/HT4312>
- Bulletin de sécurité Debian DSA-2061-1 du 16 juin 2010 :
<http://www.debian.org/security/2010/dsa-2061>
- Bulletin de sécurité HP c02627925 du 24 novembre 2010 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=0c02627925>
- Bulletin de sécurité Mandriva MDVSA-2010:119 du 17 juin 2010 :
<http://www.mandriva.com/security/advisories?name=MDVSA-2010:119>
- Bulletin de sécurité Redhat RHSA-2010:0488-1 du 16 juin 2010 :
<https://rhn.redhat.com/errata/RHSA-2010-0488.html>
- Bulletin de sécurité Suse SUSE-SR:2010:014 du 02 août 2010 :
<http://lists.opensuse.org/opensuse-security-announce/2010-08/msg00001.html>
- Bulletin de sécurité Ubuntu USN-951-1 du 16 juin 2010 :
<http://www.ubuntu.com/usn/usn-951-1>
- Référence CVE CVE-2010-2063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2063>

Gestion détaillée du document

16 juin 2010 version initiale.

29 novembre 2010 ajout des références aux bulletins des distributions.