



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 avril 2012
N° CERTA-2012-AVI-210-002

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-2012-AVI-210>

Gestion du document

Référence	CERTA-2012-AVI-210-002
Titre	Vulnérabilité dans Samba
Date de la première version	11 avril 2012
Date de la dernière version	13 avril 2012
Source(s)	Bulletin de sécurité Samba du 10 avril 2012
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 3.6.x jusqu'à la version 3.6.3 ;
- Samba 3.5.x jusqu'à la version 3.5.13 ;
- Samba 3.4.x jusqu'à la version 3.4.15.

3 Résumé

Une vulnérabilité a été corrigée dans Samba. Cette vulnérabilité est un débordement de tampon de type *heap overflow*. Elle peut être exploitée au moyen d'un message RPC, sans être authentifié et permet d'exécuter un code arbitraire à distance avec les droits *root*.

4 Solution

Les versions 3.6.4, 3.5.14 et 3.4.16 de Samba corrigent ce problème.

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

5 Documentation

- Bulletin de sécurité Samba du 10 avril 2012 :
<https://www.samba.org/samba/security/CVE-2012-1182>
- Bulletin de sécurité Debian DSA-2450 du 12 avril 2012 :
<http://www.debian.org/security/2012/dsa-2450>
- Bulletin de sécurité Mandriva MDVSA-2012:055 du 11 avril 2012 :
<http://www.mandriva.com/fr/support/security/advisories/?name=MDVSA-2012:055>
- Bulletins de sécurité RedHat RHSA-2012:0465-1 et RHSA-2012:0466-1 du 10 avril 2012 :
<https://rhn.redhat.com/errata/RHSA-2012-0465.html>
<https://rhn.redhat.com/errata/RHSA-2012-0466.html>
- Bulletin de sécurité Ubuntu USN-1423-1 du 12 avril 2012 :
<http://www.ubuntu.com/usn/usn-1423-1/>
- Référence CVE CVE-2012-1182 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1182>

Gestion détaillée du document

11 avril 2012 version initiale.

12 avril 2012 ajout des références aux bulletins Mandriva et RedHat.

13 avril 2012 précision sur les versions concernées et ajout des références aux bulletins Debian et Ubuntu.