

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Samba (SWAT)

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-2011-AVI-416>

Gestion du document

Référence	CERTA-2011-AVI-416-001
Titre	Vulnérabilités dans Samba (SWAT)
Date de la première version	28 juillet 2011
Date de la dernière version	23 août 2011
Source	Annonce de la version 3.5.10 de Samba du 26 juillet 2011
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

- Injection de code indirecte à distance ;
- injection de requêtes illégitimes par rebond.

2 Systèmes affectés

Samba Web Administration Tool (SWAT) dans les versions 3.x.

3 Résumé

La console d'administration web de Samba est vulnérable à des injections de code indirectes et à des injections de requêtes illégitimes par rebond.

4 Description

Deux vulnérabilités ont été corrigées dans la console d'administration web de Samba (SWAT) :

- (CVE-2011-2522) une injection de requêtes illégitimes par rebond (CRSF) est possible au moyen d'une URL spécialement construite ;

- (CVE-2011-2694) une injection de code indirecte est possible dans le module de changement de mots de passe.

La console SWAT n'est pas activée dans la configuration par défaut.

5 Solution

La version 3.5.10 de Samba remédie à ces problèmes.

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

6 Documentation

- Annonce de la version 3.5.10 de Samba du 26 juillet 2011 :
<http://www.samba.org/samba/history/samba-3.5.10.html>
- Bulletin de sécurité Debian DSA 2290 du 07 août 2011 :
<http://www.debian.org/security/2011/dsa-2290>
- Bulletin de sécurité Mandriva MDVSA-2011:121 du 27 juillet 2011 :
<http://www.mandriva.com/fr/support/security/advisories?name=MDVSA-2011:121>
- Bulletin de sécurité Ubuntu USN-1182-1 du 02 août 2011 :
<http://www.ubuntu.com/usn/usn-1182-1>
- Référence CVE CVE-2011-2522 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2522>
- Référence CVE CVE-2011-2694 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2694>

Gestion détaillée du document

28 juillet 2011 version initiale.

23 août 2011 ajout des références aux bulletins Debian, Mandriva et Ubuntu.