

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans auth_ldap pour Apache

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-2006-AVI-015>

Gestion du document

Référence	CERTA-2006-AVI-015-002
Titre	Vulnérabilité dans auth_ldap pour Apache
Date de la première version	10 janvier 2006
Date de la dernière version	23 janvier 2006
Source(s)	Liste des changements apportés dans la version 1.6.1 du 09 janvier 2006
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

auth_ldap versions 1.6.0 et antérieures.

3 Résumé

Une vulnérabilité dans le module pour Apache auth_ldap permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

auth_ldap permet la mise en œuvre dans Apache de l'authentification à partir d'un annuaire LDAP (Lightweight Directory Access). Un manque de contrôle du nom d'utilisateur (*username*) fourni lors de l'authentification permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un nom d'utilisateur malicieusement constitué.

5 Solution

La version 1.6.1 de `auth_ldap` corrige le problème :
http://www.rudedog.org/auth_ldap/auth_ldap-1.6.1.tar.gz

6 Documentation

- Site de l'éditeur :
http://www.rudedog.org/auth_ldap
- Liste des changements apportés dans la version 1.6.1 :
http://www.rudedog.org/auth_ldap/Changes.html
- Bulletin de sécurité RedHat RHSA-2006:0179 du 10 janvier 2006
<http://rhn.redhat.com/errata/RHSA-2006-0179.html>
- Bulletin de sécurité Mandriva MDKSA-2006:017 du 19 janvier 2006 :
<http://wwwnew.mandriva.com/security/advisories,name=MDKSA-2006:017>
- Bulletin de sécurité Debian DSA-952 du 23 janvier 2006 :
<http://www.debian.org/security/2006/dsa-952>
- Référence CVE CVE-2006-0150 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0150>

Gestion détaillée du document

10 janvier 2006 version initiale.

20 janvier 2006 ajout de la référence au bulletin de sécurité Mandriva et à la référence CVE.

23 janvier 2006 ajout des références aux bulletins de sécurité RedHat et Debian.