

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le module d'authentification pam_ldap

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-2002-AVI-242>

Gestion du document

Référence	CERTA-2002-AVI-242
Titre	Vulnérabilité dans le module d'authentification pam_ldap
Date de la première version	31 octobre 2002
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

Tout système Linux utilisant PAM avec une base d'authentification sous LDAP.

3 Résumé

PAM (« Pluggable Authentication Module ») est un système modulaire de gestion de la politique d'authentification, utilisé, entre autres, sur tous les systèmes d'exploitation Linux récents.

Un bogue dans *pam_ldap* (versions antérieures à 144) permet à un utilisateur mal intentionné d'exécuter du code malicieux.

4 Description

Parmi les divers modules, *pam_ldap* permet de gérer l'interface avec un annuaire LDAP. Cette configuration est généralement utilisée lorsque l'on souhaite centraliser les données d'authentification (comme dans le cas de NIS). Cependant un problème de chaîne de format dans le code de journalisation de ce module permet d'exécuter du code sur l'hôte réalisant l'authentification avec des privilèges élevés (généralement *root*).

5 Solution

Mettre à jour le module dans une version au moins égale à la 144.

- Linux Red Hat 6.2, 7.0, 7.1, 7.2 et 7.3
<http://rhn.redhat.com/errata/RHSA-2002-084.html>
- SCO Open Linux 3.1 et 3.1.1
<ftp://ftp.sco.com/pub/security/OpenLinux/CSSA-2002-041.0.txt>
- SuSE Linux 7.1, 7.2, 7.3 et 8.0
<http://www.suse.de/us/private/download/updates/index.html>
- Yellow Dog 2.2
<http://www.yellowdoglinux.com/resources/errata/YDU-20020606-2.txt>

6 Documentation

Avis de sécurité Blackshell

<http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0053.html>

Gestion détaillée du document

31 octobre 2002 version initiale.