

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de poppassd_pam

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-2005-AVI-013>

Gestion du document

Référence	CERTA-2005-AVI-013
Titre	Vulnérabilité de poppassd_pam
Date de la première version	13 janvier 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA-200501-22 du 11 janvier 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

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

1 Risque

- Atteinte à la confidentialité des données ;
- déni de service.

2 Systèmes affectés

- poppassd_ceti 1.0 et versions antérieures ;
- poppassd_pam 1.0 et versions antérieures.

3 Description

poppassd_pam est une bibliothèque utilisée pour modifier les mots de passes des serveurs POP.

Une vulnérabilité découverte dans la bibliothèque poppassd_pam permet à un utilisateur distant mal intentionné de changer le mot de passe de n'importe quel utilisateur du système vulnérable, y compris le mot de passe du compte root (administrateur). Cette vulnérabilité est causée par une mauvaise vérification de l'ancien mot de passe.

4 Solution

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

5 Documentation

- Bulletin de sécurité Gentoo GLSA-200501-22 du 11 janvier 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200501-22.xml>
- Référence CVE CAN-2005-0002 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0002>

Gestion détaillée du document

13 janvier 2005 version initiale.