

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de util-linux

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-359>

Gestion du document

Référence	CERTA-2005-AVI-359
Titre	Vulnérabilité de util-linux
Date de la première version	22 septembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200509-15 du 20 septembre 2005
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

Elévation de privilèges.

2 Systèmes affectés

- util-linux version stable 2.12q et versions antérieures ;
- util-linux version de développement 2.13pre2 et versions antérieures.

3 Résumé

Une vulnérabilité dans la validation des paramètres passés à l'utilitaire `umount` permet à un utilisateur mal intentionné d'élever ses privilèges.

4 Description

`util-linux` est un groupe d'utilitaires pour linux. Parmi ces utilitaires, on trouve `umount` qui sert à démonter des systèmes de fichiers.

Une vulnérabilité dans la gestion du commutateur `-r` passé à `umount` peut permettre à un utilisateur mal intentionné d'élever ses privilèges.

5 Solution

Pour la branche stable, `util-linux` version 2.12r-pre1 ou versions supérieures corrigent ces vulnérabilités. Pour la branche de développement, `util-linux` version 2.13pre3 ou versions supérieures corrigent ces vulnérabilités.

Dans tous les cas, il conviendra de se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de `util-linux` :
<http://www.kernel.org/pub/linux/utils/util-linux/>
- Bulletin de sécurité Gentoo GLSA 200509-15 du 20 septembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200509-15.xml>
- Bulletin de sécurité Mandriva MDKSA-2005:167 du 20 septembre 2005 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:167>
- Référence CVE CAN-2005-2876 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2876>

Gestion détaillée du document

22 septembre 2005 version initiale.