

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la commande `ls` sous 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-2003-AVI-180>

Gestion du document

Référence	CERTA-2003-AVI-180-004
Titre	Vulnérabilité de la commande <code>ls</code> sous Linux
Date de la première version	07 novembre 2003
Date de la dernière version	06 octobre 2005
Source(s)	Bulletin de sécurité RHSA-2003:309 de Red Hat
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

Déni de service.

2 Systèmes affectés

- Red Hat Linux 7.1, 7.2, 7.3, 8.0 et 9.0 ;
- Red Hat Enterprise Linux AS v2.1, Red Hat Enterprise Linux ES v2.1, Red Hat Enterprise Linux WS v2.1 et Red Hat Linux Advanced Workstation 2.1 pour Itanium ;
- Mandrake Linux 9.0, 9.1, 9.2, Multi Network Firewall 8.2, Corporate Server 2.1 ;
- Sun Cobalt Qube 3, Sun Cobalt RaQ 4, Sun Cobalt RaQ 550, Sun Cobalt RaQ XTR ;
- Fedora Core 1.

3 Description

Une vulnérabilité de type débordement de mémoire est présente dans la commande `/bin/ls`. Cette commande est généralement présente dans le paquetage `fileutils` des distributions Linux.

Un utilisateur malicieux peut exploiter la vulnérabilité présente dans la commande `/bin/ls` pour réaliser un déni de service par consommation excessive de ressources sur une machine vulnérable. Cette vulnérabilité est exploitable en local mais aussi à distance via un serveur `wu-ftpd` par exemple.

4 Solution

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

5 Documentation

- Avis de sécurité #62 de G. Guninski :
<http://www.guninski.com/binls.html>
- Référence CVE CAN-2003-0853 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0853>
- Référence CVE CAN-2003-0854 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0854>
- Bulletin de sécurité RedHat RHSA-2003:309 :
<http://rhn.redhat.com/errata/RHSA-2003-309.html>
- Bulletin de sécurité RedHat RHSA-2003:310 :
<http://rhn.redhat.com/errata/RHSA-2003-310.html>
- Bulletin de sécurité Mandrake MDKSA-2003:106 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:106>
- Bulletin de sécurité Fedora FEDORA-2004-091 :
<http://www.redhat.com/archives/fedora-announce-list/2004-March/msg00014.html>
- Correctifs de sécurité de Sun pour les produits Sun Cobalt Qube 3, RaQ 4, RaQ 550 et RaQ XTR :
<http://ftp.cobalt.sun.com/pub/packages/>
- Bulletin de sécurité Avaya ASA-2005-213 du 04 octobre 2005 :
<http://support.avaya.com/elmodocs2/security/ASA-2005-213.pdf>

Gestion détaillée du document

07 novembre 2003 version initiale.

14 novembre 2003 ajout du bulletin de sécurité de Mandrake Linux.

17 février 2004 ajout de la référence aux correctifs de sécurité de Sun pour les Sun Cobalt Qube3, RaQ 4, RaQ 550 et RaQ XTR.

11 mars 2004 ajout des références aux bulletins de sécurité Fedora/RedHat et ajout d'une nouvelle référence CVE.

06 octobre 2005 ajout de la références au bulletin de sécurité Avaya.