



CVE-2007-5191

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-5191
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-04 16:17:00 UTC
Updated	2023-11-07 02:01:00 UTC
Description	mount and umount in util-linux and loop-aes-utils call the setuid and setgid functions in the wrong order and do not check th

Risk And Classification

Problem Types: CWE-252

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	6.10	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Fedoraproject	Fedora	7	All	All	All
Operating System	Fedoraproject	Fedora	7	All	All	All
Application	Kernel	Util-linux	All	All	All	All
Application	Loop-aes-utils Project	Loop-aes-utils	-	All	All	All
Application	Loop-aes-utils Project	Loop-aes-utils	-	All	All	All

References

Reference
Debian update for loop-aes-utils - Advisories - Secunia

320041 – (CVE-2007-5191) CVE-2007-5191 util-linux (u)mount doesn't drop privileges properly when calling helpers
ASA-2008-023 (RHSA-2007-0969)
USN-533-1: util-linux vulnerability Ubuntu
[SECURITY] Fedora 7 Update: util-linux-2.13-0.54.1.fc7
rPath update for util-linux - Advisories - Secunia
Webmail- OVH
VMSA-2008-0001.1 - VMware
VMware ESX Server Multiple Security Updates - Advisories - Secunia
Debian -- Security Information -- DSA-1449-1 loop-aes-utils
SecurityFocus
issues.rpath.com/browse/RPL-1757
Support
git.kernel.org
[Security-announce] VMSA-2008-0001 Moderate OpenPegasus PAM Authentication Buffer Overflow and updated service console packages
git.kernel.org
Gentoo update for util-linux - Advisories - Secunia
Gentoo Bug 195390 - sys-apps/util-linux < 2.12r-r8 Privilege Escalation Vulnerability (CVE-2007-5191)
Repository / Oval Repository
Avaya Products util-linux Privilege Escalation Vulnerability - Advisories - Secunia
Ubuntu update for util-linux - Advisories - Secunia
Debian update for util-linux - Advisories - Secunia
SUSE Update for Multiple Packages - Advisories - Secunia
SecurityTracker.com Archives - Util-linux mount/umount Privilege Bug Lets Local Users Gain Elevated Privileges
Webmail - OVH
Mandriva update for util-linux - Advisories - Secunia
[security-announce] SUSE Security Summary Report SUSE-SR:2007:022
Gentoo Linux Documentation -- util-linux: Local privilege escalation
Red Hat update for util-linux - Advisories - Secunia
util-linux mount umount Local Privilege Escalation Vulnerability
util-linux Privilege Escalation Vulnerability - Advisories - Secunia
Fedora update for util-linux - Advisories - Secunia
SecurityFocus
Advisories Mandriva
Debian -- Security Information -- DSA-1450-1 util-linux
CVE Program record
ANNOUNCEMENT: CVE-2007-5191

Vendor Comments And Credit

Organization	Published	Contributor	Statement
--------------	-----------	-------------	-----------

Red Hat	2009-06-01	Mark J Cox	Updates are available to address this issue: https://rhn.redhat.com/errata/RHSA-2007-0969.htm
---------	------------	------------	--

Legacy QID Mappings

900176 CBL-Mariner Linux Security Update for util-linux 2.32.1

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report