



CVE-2005-3179

Published on: 10/11/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:23 PM UTC

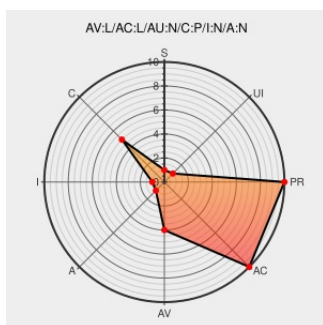
CVE-2005-3179

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

drm.c in Linux kernel 2.6.10 to 2.6.13 creates a debug file in sysfs with world-readable and world-writable permissions, which allows local users to enable DRM debugging and obtain sensitive information.

CVE-2005-3179 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Secunia - Advisories - Linux Kernel
Potential Denial of Service and
Information Disclosure

Permissions Required
Third Party Advisory
web.archive.org
text/html

SECUNIA 17114

Advisories - Mandriva Linux

Broken Link
www.mandriva.com
text/html

MANDRIVA MDKSA-2005:235

Secunia - Advisories - Fedora update
for kernel

Permissions Required
Third Party Advisory
web.archive.org
text/html

SECUNIA 17280

Linux Kernel World Writable SYSFS
DRM Debug File Vulnerability

Third Party Advisory
VDB Entry
cve.report (archive)

BID 15154

	CVEreport (archive) text/html	
Advisory: Fedora Core 3 Update: kernel-2.6.12-1.1380_FC3	Third Party Advisory VDB Entry web.archive.org text/html Inactive Link Not Archived	 FEDORA FEDORA-2005-1007
Gentoo Bug 107893 - sysfs world writable file: /sys/module/drm/parameters/debug	Patch Vendor Advisory bugs.gentoo.org text/html	 CONFIRM bugs.gentoo.org/show_bug.cgi?id=107893
Advisories - Mandriva Linux	www.mandriva.com text/html	 MANDRAKE MDKSA-2005:220
Linux 2.6: changeset d7067d7d1f92	Patch web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.kernel.org/hg/linux-2.6/?cmd=changeset;node=d7067d7d1f92cba14963a430cfbd53098cbbc8fd
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All

Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating Svstem	Linux	Linux Kernel	2.6.11.7	All	All	All

Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.12:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*****:						

cpe:2.3:o:linux:linux_kernel:2.6.12.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.13:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)