

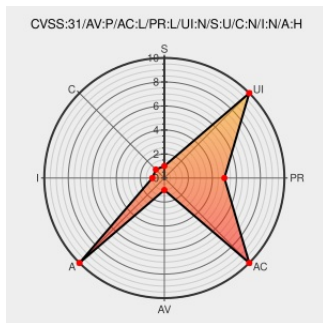


CVE-2010-5321

Published on: 04/24/2017 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:22:00 AM UTC

CVE-2010-5321

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux kernel 2.6.x through 4.x allows local users to cause a denial of service (memory consumption) by leveraging /dev/video access for a series of mmap calls that require new allocations, a different vulnerability than CVE-2007-6761. NOTE: as of

2016-06-18, this affects only 11 drivers that have not been updated to use videobuf2 instead of videobuf.

CVE-2010-5321 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
#892340 - linux CVE-2010-5321 memory leak in videobuf-core	Linux Kernel	MISC bugs.debian.org/cgi-bin/bugreport.cgi?

#827340 - linux: CVE-2010-5321 memory leak in videobuf on multiple calls to mmap() - Debian Bug report logs	Issue Tracking Mailing List Third Party Advisory bugs.debian.org text/html	 MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=827340
620629 – (CVE-2010-5321) CVE-2010-5321 kernel: v4l: videobuf: hotfix a bug on multiple calls to mmap()	Issue Tracking Third Party Advisory VDB Entry bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=620629
120571 – CVE-2010-5321 Multiple mmap() calls to v4l drivers using videobuf leak memory	Issue Tracking Third Party Advisory VDB Entry bugzilla.kernel.org text/html	 MISC bugzilla.kernel.org/show_bug.cgi?id=120571
oss-security - Re: kernel: v4l: videobuf: hotfix a bug on multiple calls to mmap() - Linux kernel	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20150208 Re: kernel: v4l: videobuf: hotfix a bug on multiple calls to mmap() - Linux kernel
IRC Log for on , collected by	Not Applicable linuxtv.org text/html	 MISC linuxtv.org/irc/v4l/index.php?date=2010-07-29

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	All	All	All	All
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						

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](#)