



CVE-2016-4568

Published on: 05/23/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:39:00 PM UTC

CVE-2016-4568

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call.

CVE-2016-4568 has been assigned by security@debian.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
oss-security - CVE Request: Linux: [media] videobuf2-v4l2: Verify planes array in buffer dequeuing	www.openwall.com text/html	MLIST [oss-security] 20160507 CVE Request: Linux: [media] videobuf2-v4l2: Verify planes array in buffer dequeuing

[www.kernel.org](#)
[text/plain](#)

CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.3

[media] videobuf2-v4l2: Verify planes array in buffer dequeuing · torvalds/linux@2c1f695 · GitHub

Vendor Advisory

[github.com](#)

[text/html](#)

CONFIRM github.com/torvalds/linux/commit/2c1f6951a8a82e6de0d82b1158b5e493fc6c54ab

kernel/git/torvalds/linux.git - Linux kernel source tree

[git.kernel.org](#)

[text/html](#)

CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2c1f6951a8a82e6de0d82b1158b5e493fc6c54ab

1334316 – (CVE-2016-4568) CVE-2016-4568 kernel: videobuf2-v4l2: Planes array amount not verified in buffer dequeuing

[bugzilla.redhat.com](#)

[text/html](#)

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1334316

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
Operating System	Linux	Linux Kernel	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →