

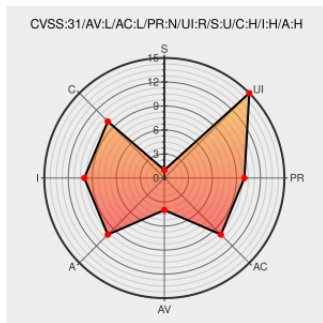


CVE-2016-7911

Published on: 11/15/2016 12:00:00 AM UTC

Last Modified on: 01/19/2023 04:05:00 PM UTC

CVE-2016-7911

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

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

Race condition in the `get_task_ioprio` function in `block/ioprio.c` in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted `ioprio_get` system call.

CVE-2016-7911 has been assigned by security@android.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Android Security Bulletin—November 2016 Android Open Source Project	Third Party Advisory source.android.com text/html	CONFIRM source.android.com/security/bulletin/2016-11-01.html
Linux kernel Local Use After	cve.report (archive)	BID 94135

Free Multiple Denial of Service Vulnerabilities

text/html

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

Issue Tracking

Patch

Third Party Advisory

git.kernel.org

text/x-c

CONFIRM

git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=8ba8682107ee2ca3347354e018865d8e1967c5f4

block: fix use-after-free in sys_ioprio_get() · torvalds/linux@8ba8682 · GitHub

Issue Tracking

Patch

Third Party Advisory

github.com

text/html

CONFIRM

github.com/torvalds/linux/commit/8ba8682107ee2ca3347354e018865d8e1967c5f4

Release Notes

Vendor Advisory

www.kernel.org

text/plain

CONFIRM

www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.6.6

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