

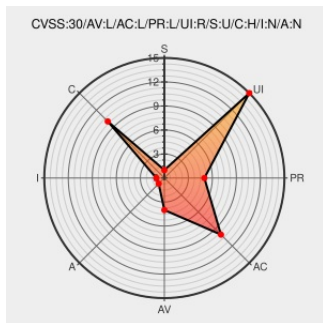


CVE-2016-7917

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

Last Modified on: 03/23/2021 11:27:06 PM UTC

CVE-2016-7917

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

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

The `nfnetlink_rcv_batch` function in `net/netfilter/nfnetlink.c` in the Linux kernel before 4.5 does not check whether a batch message's length field is large enough, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (infinite loop or out-of-bounds read) by leveraging the `CAP_NET_ADMIN`

capability.

CVE-2016-7917 has been assigned by security@android.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Android Security Bulletin—November 2016 Android Open	Third Party Advisory source.android.com	CONFIRM source.android.com/security/bulletin/2016-11-01.html

Source Project	text/html	
netfilter: nfnetlink: correctly validate length of batch messages · torvalds/linux@c58d6c9 · GitHub	Issue Tracking Patch github.com text/html	 CONFIRM github.com/torvalds/linux/commit/c58d6c93680f28ac58984af61d0a7ebf4319c241
Google Android Kernel Components Multiple Information Disclosure Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 94147
kernel/git/torvalds/linux.git - Linux kernel source tree	Issue Tracking Patch Third Party Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c58d6c93680f28ac58984af61d0a7ebf4319c241

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
<code>cpe:2.3:o:linux:linux_kernel:*****:</code>						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)