

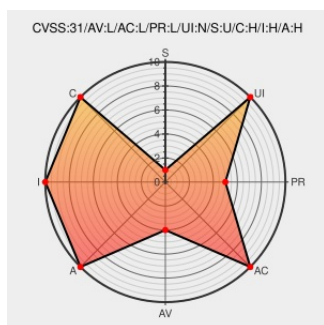


CVE-2016-9806

Published on: 12/28/2016 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:05:00 PM UTC

CVE-2016-9806

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

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

Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than

anticipated.

CVE-2016-9806 has been assigned by [M](#) cve@mitre.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
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2017:1842

Linux Kernel CVE-2016-9806 Local Denial of Service Vulnerability	cve.report (archive) text/html	 BID 94653
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2017:2669
	Release Notes www.kernel.org text/plain	 CONFIRM www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.6.3
Android Security Bulletin— March 2017 Android Open Source Project	source.android.com text/html	 CONFIRM source.android.com/security/bulletin/2017-03-01.html
netdev - BUG: use-after-free in netlink_dump	Mailing List lists.openwall.net text/html	 MLIST [netdev] 20160515 BUG: use-after-free in netlink_dump
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 CONFIRM git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=92964c79b357efd980812c4de5c1fd2ec8bb5520
Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remote Users Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1037968
Bug 1401502 – CVE-2016- 9806 kernel: netlink: double- free in netlink_dump	Issue Tracking Patch bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1401502
oss-security - CVE Request: -- Linux kernel: double free in netlink_dump	Mailing List Patch www.openwall.com text/html	 MLIST [oss-security] 20161203 CVE Request: -- Linux kernel: double free in netlink_dump
netlink: Fix dump skb leak/double free · torvalds/linux@92964c7 · GitHub	Patch github.com text/html	 CONFIRM github.com/torvalds/linux/commit/92964c79b357efd980812c4de5c1fd2ec8bb5520
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2017:2077

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	Linux	Linux Kernel	All	All	All	All

Operating System	Linux	Linux Kernel	All	All	All	All
<pre>cpe:2.3:o:linux:linux_kernel:*****:</pre>						
<pre>cpe:2.3:o:linux:linux_kernel:*****:</pre>						

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