

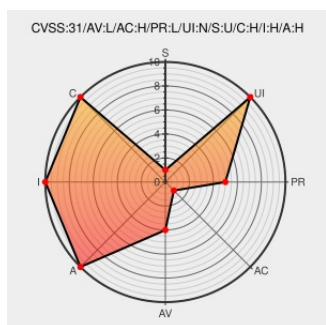


CVE-2017-17712

Published on: 12/15/2017 12:00:00 AM UTC

Last Modified on: 06/21/2023 09:01:00 PM UTC

CVE-2017-17712

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

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

The `raw_sendmsg()` function in `net/ipv4/raw.c` in the Linux kernel through 4.14.6 has a race condition in `inet->hdrincl` that leads to uninitialized stack pointer usage; this allows a local user to execute code and gain privileges.

CVE-2017-17712 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7 - HIGH**

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

CVSS2 Score: **6.9 - MEDIUM**

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

CVE References

Description	Tags	Link
net: ipv4: fix for a race condition in <code>raw_sendmsg</code> · torvalds/linux@8f659a0 · GitHub	Patch github.com text/html	github.com/torvalds/linux/commit/8f659a03a0ba9289b9aeb9b4470e6fb263d6f483
USN-3581-3: Linux kernel	usn.ubuntu.com	UBUNTU USN-3581-3

(Raspberry Pi 2) vulnerabilities Ubuntu security notices Ubuntu	text/html	
USN-3582-2: Linux kernel (Xenial HWE) vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3582-2
USN-3582-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3582-1
USN-3581-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3581-1
Pixel/Nexus Security Bulletin—April 2018 Android Open Source Project	source.android.com text/html	 CONFIRM source.android.com/security/bulletin/pixel/2018-04-01
Debian -- Security Information -- DSA-4073-1 linux	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4073
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2018:0502
USN-3581-2: Linux kernel (HWE) vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-3581-2
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch git.kernel.org text/html	 CONFIRM git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483

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

© [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](#)