

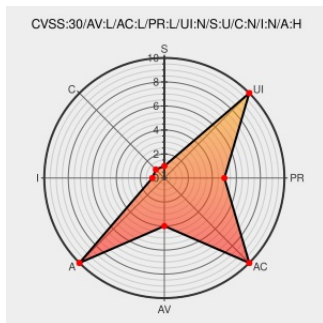


CVE-2018-14646

Published on: 11/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:43 PM UTC

CVE-2018-14646

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

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

The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the `__netlink_ns_capable()` function in the `net/netlink/af_netlink.c` file. A local attacker could exploit this when a net namespace with a netnsid is assigned to cause a kernel panic and a denial of service.

CVE-2018-14646 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **[UNKNOWN]** - **kernel:** version **4.15-rc8**

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **4.9 - MEDIUM**

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source	Patch	CONFIRM

tree	Third Party Advisory git.kernel.org text/html	git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f428fe4a04cc339166c8bbd489789760de3a0cee
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3666
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3651
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	 REDHAT RHSA-2018:3843
1630124 – (CVE-2018-14646) CVE-2018-14646 kernel: NULL pointer dereference in af_netlink.c: __netlink_ns_capable() allows for denial of service	Issue Tracking Patch Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14646
'[PATCH v2] rtnetlink: give a user socket to get_target_net()' - MARC	Patch Third Party Advisory marc.info text/x-diff	 CONFIRM marc.info/?l=linux-netdev&m=151500466401174&w=2

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	4.15	rc1	All	All
Operating System	Linux	Linux Kernel	4.15	rc2	All	All
Operating System	Linux	Linux Kernel	4.15	rc3	All	All
Operating System	Linux	Linux Kernel	4.15	rc4	All	All
Operating System	Linux	Linux Kernel	4.15	rc5	All	All
Operating System	Linux	Linux Kernel	4.15	rc6	All	All
Operating System	Linux	Linux Kernel	4.15	rc7	All	All
Operating System	Linux	Linux Kernel	4.15	rc1	All	All
Operating System	Linux	Linux Kernel	4.15	rc2	All	All

cpe:2.3:o:linux:linux_kernel:4.15:rc4:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc5:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc6:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc7:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc1:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc2:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc3:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc4:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc5:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc6:*****:
cpe:2.3:o:linux:linux_kernel:4.15:rc7:*****:
cpe:2.3:o:linux:linux_kernel:*****:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*****:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*****:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*****:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*****:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*****:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:*****:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6:*****:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*****:

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](#)