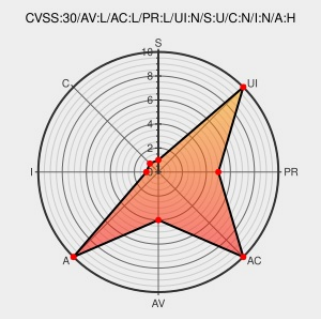
CVE-2018-14646

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

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

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	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

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: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→