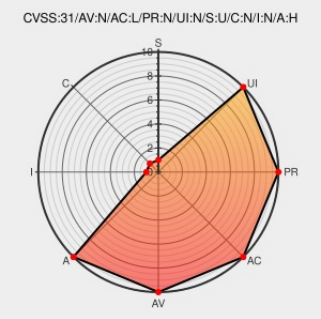
CVE-2019-18680

Published on: 11/04/2019 12:00:00 AM UTC

Last Modified on: 01/17/2023 09:31:00 PM UTC

CVE-2019-18680

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

An issue was discovered in the Linux kernel 4.4.x before 4.4.195. There is a NULL pointer dereference in rds_tcp_kill_sock() in net/rds/tcp.c that will cause denial of service, aka CID-91573ae4aed0.

CVE-2019-18680 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
November 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20191205-0001/

	Exploit Patch Vendor Advisory cdn.kernel.org text/plain	MISC cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.195
LKML: Mao Wenan: [PATCH stable 4.4 net] net: rds: Fix NULL ptr use in rds_tcp_kill_sock	Exploit Mailing List Vendor Advisory lkml.org text/xml	MISC lkml.org/lkml/2019/9/18/337
kernel/git/stable/linux.git - Linux kernel stable tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=91573ae4aed0a49660abdad4d42f2a0db995ee5e
net: rds: Fix NULL ptr use in rds_tcp_kill_sock · torvalds/linux@91573ae · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/91573ae4aed0a49660abdad4d42f2a0db995ee5e

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

← Previous ID

Next ID→