

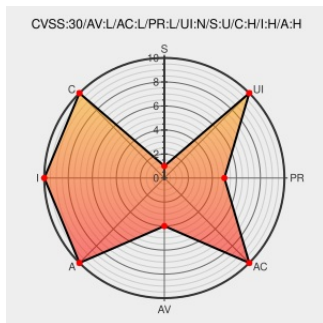


CVE-2018-20854

Published on: 07/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:36 PM UTC

CVE-2018-20854

[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 before 4.20. drivers/phy/mscc/phy-ocelot-serdes.c has an off-by-one error with a resultant ctrl->phys out-of-bounds read.

CVE-2018-20854 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: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=6acb47d1a318e5b3b7115354ebc4ea060c59d3a1

No Description Provided

support.f5.com

text/html

CONFIRM support.f5.com/csp/article/K32450233

No Description Provided

support.f5.com

text/html

CONFIRM support.f5.com/csp/article/K32450233?utm_source=f5support&utm_medium=RSS

phy: ocelot-serdes: fix out-of-bounds read ·
torvalds/linux@6acb47d ·
GitHub

Patch

Third Party Advisory

github.com

text/html

MISC
github.com/torvalds/linux/commit/6acb47d1a318e5b3b7115354ebc4ea060c59d3a1

August 2019 Linux Kernel Vulnerabilities in NetApp Products | NetApp Product Security

security.netapp.com

text/html

CONFIRM security.netapp.com/advisory/ntap-20190905-0002/

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 →