



CVE-2019-19081

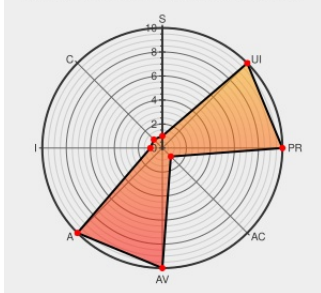
Published on: 11/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19081

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

A memory leak in the `nfp_flower_spawn_vnic_reprs()` function in `drivers/net/ethernet/netronome/nfp/flower/main.c` in the Linux kernel before 5.3.4 allows attackers to cause a denial of service (memory consumption), aka CID-8ce39eb5a67a.

CVE-2019-19081 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

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

CVSS2 Score: **7.1 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	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	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20191205-0001/

 [MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.4](https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.4)

text/plain

text/html

github.com/torvalds/linux/commit/8ce39eb5a67aee25d9f05b40b673c95b23502e3e

There are currently no QIDs associated with this CVE

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
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
cpe:2.3:o:linux:linux_kernel:*****:.*:						
cpe:2.3:o:linux:linux_kernel:*****:.*:						
cpe:2.3:o:opensuse:leap:15.1:*****:.*:						
cpe:2.3:o:opensuse:leap:15.1:*****:.*:						
cpe:2.3:o:redhat:enterprise_linux:7.0:*****:.*:						
cpe:2.3:o:redhat:enterprise_linux:8.0:*****:.*:						
cpe:2.3:o:redhat:enterprise_linux:7.0:*****:.*:						

ΟΡΘΟΓΩΝΙΑΣ ΤΩΝ ΕΠΙΠΕΔΩΝ ΕΠΙΧΕΙΡΗΣΗΣ

```
cpe:2.3:o:redhat:enterprise_linux:8.0:*:*:*:*:
```

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