



CVE-2019-19070

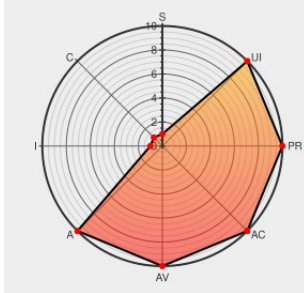
Published on: 11/18/2019 12:00:00 AM UTC

Last Modified on: 06/02/2021 03:38:00 PM UTC

CVE-2019-19070

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

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



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

**** DISPUTED **** A memory leak in the `spi_gpio_probe()` function in `drivers/spi/spi-gpio.c` in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering `devm_add_action_or_reset()` failures, aka CID-d3b0ffa1d75d. NOTE: third parties dispute the relevance of this

because the system must have already been out of memory before the probe began.

CVE-2019-19070 has been assigned by [M](#) 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
[SECURITY] Fedora 31 Update: kernel-5.3.12-300.fc31 -	lists.fedoraproject.org text/html	FEDORA FEDORA-2019-34a75d7e61

package-announce - Fedora
Mailing-Lists

Bug 1157294 – VUL-1:
DISPUTED: CVE-2019-19070:
kernel-source: memory leak in
the spi_gpio_probe() function in
drivers/spi/spi-gpio.c

bugzilla.suse.com
text/html

MISC bugzilla.suse.com/show_bug.cgi?id=1157294

[SECURITY] Fedora 30 Update:
kernel-5.3.12-200.fc30 -
package-announce - Fedora
Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2019-021c968423

spi: gpio: prevent memory leak
in spi_gpio_probe ·
torvalds/linux@d3b0ffa · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/torvalds/linux/commit/d3b0ffa1d75d5305e34735598993afbb8a869d

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	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.5	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:fedoraproject:fedora:30:*****:						
cpe:2.3:o:fedoraproject:fedora:31:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:5.5:rc1:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← 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](#)