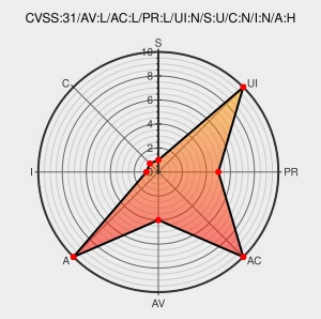
CVE-2021-4150

Published on: Not Yet Published

Last Modified on: 06/22/2022 03:55:00 PM UTC

CVE-2021-4150

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



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

A use-after-free flaw was found in the add_partition in block/partitions/core.c in the Linux kernel. A local attacker with user privileges could cause a denial of service on the system. The issue results from the lack of code cleanup when device_add call fails when adding a partition to the disk.

CVE-2021-4150 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

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
LKML: Hao Sun: WARNING in __init_work	lkml.org text/xml	MISC lkml.org/lkml/2021/9/6/781
2025938 – (CVE-2021-4150) CVE-2021-4150 kernel: Block subsystem	bugzilla.redhat.com	MISC

mishandles reference counts	text/html	bugzilla.redhat.com/show_bug.cgi?id=2025938
	lkml.org text/plain Inactive Link Not Archived	MISC lkml.org/lkml/2021/10/18/485

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.

Related QID Numbers

900781 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9137)

902031 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9137-1)

906067 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9137-2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux	Linux Kernel	All	All	All	All
Application	Linux	Linux Kernel	5.15	All	All	All
Application	Linux	Linux Kernel	5.15	rc1	All	All
Application	Linux	Linux Kernel	5.15	rc2	All	All
Application	Linux	Linux Kernel	5.15	rc3	All	All
Application	Linux	Linux Kernel	5.15	rc4	All	All
Application	Linux	Linux Kernel	5.15	rc5	All	All
Application	Linux	Linux Kernel	5.15	rc6	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.15	All	All	All
Operating System	Linux	Linux Kernel	5.15	rc1	All	All
Operating System	Linux	Linux Kernel	5.15	rc2	All	All
Operating System	Linux	Linux Kernel	5.15	rc3	All	All
Operating System	Linux	Linux Kernel	5.15	rc4	All	All
Operating System	Linux	Linux Kernel	5.15	rc5	All	All
Operating System	Linux	Linux Kernel	5.15	rc6	All	All

cpe:2.3:a:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:*:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc1:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc2:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc3:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc4:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc5:*:*:*:*:*:*:

cpe:2.3:a:linux:linux_kernel:5.15:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:5.15:rc6:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-4150 : A use-after-free flaw was found in the add_partition in block/partitions/core.c in the #Linux… twitter.com/i/web/status/1…	2022-03-23 20:16:58

← 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 registred 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