



# CVE-2021-4149

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-4149
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-23 20:15:00 UTC
<b>Updated</b>	2023-02-01 15:53:00 UTC
<b>Description</b>	A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock operation

## Risk And Classification

**Problem Types:** CWE-667

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	-	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc1	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc2	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc3	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc4	All	All
Application	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc5	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	-	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc1	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc2	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc3	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc4	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	5.15	rc5	All	All

## References

Reference	Source	Link
-----------	--------	------

LKML: Hao Sun: WARNING: lock held when returning to user space in __btrfs_tree_lock	MISC	<a href="https://lkml.org">lkml.org</a>
LKML: Greg Kroah-Hartman: [PATCH 5.14 030/151] btrfs: unlock newly allocated extent buffer after error	MISC	<a href="https://lkml.org">lkml.org</a>
2026485 – (CVE-2021-4149) CVE-2021-4149 kernel: Improper lock operation in btrfs	MISC	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
[SECURITY] [DLA 3065-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159760](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9314)

[159763](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9313)

[159777](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9348)

[179840](#) Debian Security Update for linux (CVE-2021-4149)

[180282](#) Debian Security Update for linux (DLA 3065-1)

[198825](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5466-1)

[199560](#) Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6001-1)

[199568](#) Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6013-1)

[199577](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6014-1)

[390261](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2022-0014)

[671703](#) EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

[751602](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0080-1)

[751654](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0197-1)

[751657](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0198-1)

[751666](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0169-1)

[751695](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0367-1)

[751696](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0364-1)

[751697](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0366-1)

[751698](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0362-1)

[751701](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2022:0366-1)

[751700](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0371-1)

<a href="#">751702</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:03/1-1)
<a href="#">751993</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0198-1)
<a href="#">753194</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0288-1)
<a href="#">753267</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0169-1)
<a href="#">753462</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:0289-1)
<a href="#">900780</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9136)
<a href="#">901316</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9136-1)
<a href="#">905972</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9136-2)

© [CVE.report](#) 2026 |

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](#)**