



# CVE-2021-34693

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

## Summary

<b>CVE</b>	CVE-2021-34693
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-06-14 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:36:00 UTC
<b>Description</b>	net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memo

## Risk And Classification

**Problem Types:** CWE-909

## 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>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 2713-2] linux security update	MLIST	<a href="#">lists.debian.org</a>	
[SECURITY] [DLA 2713-1] linux security update	MLIST	<a href="#">lists.debian.org</a>	
oss-security - CVE-2021-34693: Infoleak in CAN BCM protocol in Linux kernel	MLIST	<a href="#">www.openwall.com</a>	
[PATCH] can: bcm: fix infoleak in struct bcm_msg_head	MISC	<a href="#">lore.kernel.org</a>	
Debian -- Security Information -- DSA-4941-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
[PATCH] can: bcm: fix infoleak in struct bcm_msg_head		<a href="#">lore.kernel.org</a>	
[SECURITY] [DLA 2714-1] linux-4.19 security update	MLIST	<a href="#">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159380](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9442)

[159399](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9452)

[159400](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9453)

[178710](#) Debian Security Update for linux (DSA 4941-1)

[178712](#) Debian Security Update for linux (DLA 2713-1)

[178713](#) Debian Security Update for linux-4.19 (DLA 2714-1)

[178714](#) Debian Security Update for linux (DLA 2713-2)

[179953](#) Debian Security Update for linux (CVE-2021-34693)

[198464](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5045-1)

[198491](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5070-1)

[198497](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5073-1)

[198506](#) Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-5073-2)

[198507](#) Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5073-3)

[353097](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-033

[353098](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-034

[353099](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-035

[353147](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004

[353158](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002

[390219](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0030)

[670707](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2465)

[670744](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2502)

[670772](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2530)

[670796](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2554)

[671047](#) EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

[750828](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2305-1)

[750830](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2321-1)

[750832](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2324-1)

<a href="#">750842</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2352-1)
<a href="#">750864</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)
<a href="#">750868</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2427-1)
<a href="#">750869</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2422-1)
<a href="#">750877</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2427-1)
<a href="#">750880</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2451-1)
<a href="#">900096</a> CBL-Mariner Linux Security Update for kernel 5.10.52.1
<a href="#">900304</a> CBL-Mariner Linux Security Update for kernel 5.10.57.1
<a href="#">900319</a> CBL-Mariner Linux Security Update for kernel 5.10.60.1
<a href="#">901049</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6567-1)
<a href="#">903698</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4361)
<a href="#">905973</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4361-1)

© [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](#)**