



# CVE-2022-4129

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-4129
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-11-28 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:57:00 UTC
<b>Description</b>	A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing sk_user_data can l

## 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="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Linux</a>	<a href="#">Layer 2 Tunneling Protocol</a>	All	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] Fedora 36 Update: kernel-6.0.11-200.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[PATCH net v2] l2tp: Don't sleep and disable BH under writer-side sk_callback_lock	MISC	<a href="https://lore.kernel.org">lore.kernel.org</a>	
[SECURITY] Fedora 35 Update: kernel-6.0.11-100.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[PATCH net v2] l2tp: Don't sleep and disable BH under writer-side sk_callback_lock	MISC	<a href="https://lore.kernel.org">lore.kernel.org</a>	
[SECURITY] Fedora 35 Update: kernel-6.0.11-100.fc35 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] [DLA 3404-1] linux-5.10 security update	MISC	<a href="https://lists.debian.org">lists.debian.org</a>	
[PATCH net v4] l2tp: Serialize access to sk_user_data with sk_callback_lock	MISC	<a href="https://lore.kernel.org">lore.kernel.org</a>	
[SECURITY] Fedora 37 Update: kernel-6.0.11-300.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: kernel-6.0.11-300.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 36 Update: kernel-6.0.11-200.fc36 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	

[PATCH net v4] l2tp: Serialize access to sk_user_data with sk_callback_lock	MISC	<a href="https://lore.kernel.org">lore.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[160505](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12196)

[160551](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-12256)

[160554](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-12255)

[160583](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2458)

[160692](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-2951)

[181765](#) Debian Security Update for linux-5.10 (DLA 3404-1)

[183535](#) Debian Security Update for linux (CVE-2022-4129)

[199292](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6025-1)

[199301](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6027-1)

[199303](#) Ubuntu Security Notification for Linux kernel (HWE) Vulnerabilities (USN-6040-1)

[199321](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6057-1)

[199343](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6079-1)

[199353](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6091-1)

[199354](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6096-1)

[199356](#) Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-6093-1)

[199385](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6134-1)

[199465](#) Ubuntu Security Notification for Linux kernel (Xilinx ZynqMP) Vulnerabilities (USN-6222-1)

[199614](#) Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6256-1)

[241417](#) Red Hat Update for kernel security (RHSA-2023:2458)

[241468](#) Red Hat Update for kernel-rt (RHSA-2023:2148)

[241504](#) Red Hat Update for kernel security (RHSA-2023:2951)

[241527](#) Red Hat Update for kernel-rt (RHSA-2023:2736)

[242855](#) Red Hat Update for kernel (RHSA-2024:0412)

<a href="#">283382</a> Fedora Security Update for kernel (FEDORA-2022-24041b1667)
<a href="#">283383</a> Fedora Security Update for kernel (FEDORA-2022-b36cd53dca)
<a href="#">283390</a> Fedora Security Update for kernel (FEDORA-2022-e4460c41bc)
<a href="#">354775</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-042
<a href="#">354829</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-027
<a href="#">354831</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-014
<a href="#">378468</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
<a href="#">378473</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)
<a href="#">378512</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
<a href="#">6140121</a> AWS Bottlerocket Security Update for kernel (GHSA-6mjp-35gq-h9v5)
<a href="#">672595</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1320)
<a href="#">672653</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1388)
<a href="#">672675</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1409)
<a href="#">672687</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1424)
<a href="#">672806</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1526)
<a href="#">673117</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2152)
<a href="#">753020</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4585-1)
<a href="#">753034</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4504-1)
<a href="#">753045</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4503-1)
<a href="#">753051</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)
<a href="#">753061</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4616-1)
<a href="#">753062</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4613-1)
<a href="#">753063</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
<a href="#">753801</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0762-1)
<a href="#">753806</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0770-1)
<a href="#">753807</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0768-1)
<a href="#">753832</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0852-1)
<a href="#">941023</a> AlmaLinux Security Update for kernel (ALSA-2023:2458)

941061 AlmaLinux Security Update for kernel-rt (ALSA-2023:2148)

941096 AlmaLinux Security Update for kernel (ALSA-2023:2951)

941114 AlmaLinux Security Update for kernel-rt (ALSA-2023:2736)

© [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](#)**