



CVE-2022-3565

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

Summary

CVE	CVE-2022-3565
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-17 19:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_tim

Risk And Classification

Problem Types: CWE-662

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All

References

Reference	Source	Link	Tags
kernel/git/bluetooth/bluetooth-next.git - Bluetooth kernel development tree	MISC	git.kernel.org	
[SECURITY] [DLA 3245-1] linux security update	MLIST	lists.debian.org	
CVE-2022-3565 Linux Kernel Bluetooth l1oip_core.c del_timer use after free	MISC	vuldb.com	
[SECURITY] [DLA 3244-1] linux-5.10 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160345](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-10065)

[160351](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-10081)

160353 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-10072)
160354 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-10079)
160355 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-10073)
161066 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-6583)
181354 Debian Security Update for linux (CVE-2022-3565)
181440 Debian Security Update for linux-5.10 (DLA 3244-1)
181565 Debian Security Update for linux (DLA 3245-1)
199055 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5754-1)
199056 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5757-1)
199057 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5755-1)
199059 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5756-1)
199060 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-5756-2)
199061 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5755-2)
199070 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5756-3)
199071 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5754-2)
199072 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5774-1)
199078 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5779-1)
199210 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5913-1)
242399 Red Hat Update for kernel security (RHSA-2023:6583)
354239 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-023
354251 Amazon Linux Security Advisory for kernel : ALAS-2022-1645
354275 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-039
377891 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0002)
378043 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0011)
378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)
378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)
390269 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0031)
6140273 AWS Bottlerocket Security Update for kernel (GHSA-6c8j-mxvp-xgcp)
676416 Fedora Security Update for kernel (FUS-2023-0750)

672410 EulerOS Security Update for kernel (EulerOS-SA-2022-2796)
672532 EulerOS Security Update for kernel (EulerOS-SA-2023-1126)
672653 EulerOS Security Update for kernel (EulerOS-SA-2023-1388)
672711 EulerOS Security Update for kernel (EulerOS-SA-2023-1507)
752813 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3930-1)
752839 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3929-1)
752880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4053-1)
752889 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3897-1)
752911 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3998-1)
752913 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4072-1)
752944 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4273-1)
752959 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4272-1)
753038 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4573-1)
753039 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4574-1)
753051 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4589-1)
753060 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4615-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753703 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753707 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)
753727 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:0416-1)

© [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](#)