



CVE-2022-1966

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

Summary

CVE	CVE-2022-1966
State	REJECT
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-06 18:15:00 UTC
Updated	2023-11-07 03:42:00 UTC
Description	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a dup

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

References

Reference

- [SECURITY] Fedora 35 Update: kernel-5.17.13-200.fc35 - package-announce - Fedora Mailing-Lists
- [kernel/git/netdev/net.git](#) - Netdev Group's networking tree
- [SECURITY] Fedora 36 Update: kernel-5.17.13-300.fc36 - package-announce - Fedora Mailing-Lists
- [oss-security](#) - Linux Kernel use-after-free write in netfilter
- Debian -- Security Information -- DSA-5161-1 linux
- 2092427 – (CVE-2022-1966) CVE-2022-1966 kernel: a use-after-free write in the netfilter subsystem can lead to privilege escalation to root
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159915 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5232)
159931 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5249)
179371 Debian Security Update for linux (DSA 5161-1)
198821 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5470-1)
198822 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5469-1)
198823 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5471-1)
198824 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5467-1)
198825 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5466-1)
198826 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5468-1)
240484 Red Hat Update for kernel-rt (RHSA-2022:5236)
240485 Red Hat Update for kernel (RHSA-2022:5232)
240487 Red Hat Update for kpatch-patch (RHSA-2022:5214)
240490 Red Hat Update for kpatch-patch (RHSA-2022:5216)
240494 Red Hat Update for kernel (RHSA-2022:5220)
240499 Red Hat Update for kernel (RHSA-2022:5249)
240524 Red Hat Update for kpatch-patch (RHSA-2022:5476)
240527 Red Hat Update for kernel-rt (RHSA-2022:5267)
240531 Red Hat Update for kernel-rt (RHSA-2022:5224)
257172 CentOS Security Update for kernel (CESA-2022:5232)
282812 Fedora Security Update for kernel (FEDORA-2022-80cc9873be)
282813 Fedora Security Update for kernel (FEDORA-2022-8269eaf361)
353976 Amazon Linux Security Advisory for kernel : ALAS-2022-1604
353985 Amazon Linux Security Advisory for kernel : ALAS2-2022-1813
353991 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-083
353992 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-082
353993 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-016

353994 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-028
353995 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-079
353998 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-081
353999 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-078
354003 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-080
354007 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-015
354008 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-030
354012 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-086
354015 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-085
354017 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-032
354018 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-003
354022 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-002
354023 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-017
354024 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-004
354026 Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2022-084
354270 Amazon Linux Security Advisory for kernel : ALAS2022-2022-114
354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185
354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185
355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070
377117 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)
672017 EulerOS Security Update for kernel (EulerOS-SA-2022-2244)
672037 EulerOS Security Update for kernel (EulerOS-SA-2022-2257)
752234 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2080-1)
752242 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2104-1)
752254 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2116-1)
752276 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2173-1)
752370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
753091 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2172-1)
753148 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)

753153	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP3) (SUSE-SU-2022:2239-1)
753169	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP2) (SUSE-SU-2022:2230-1)
753243	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:2216-1)
753253	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:2245-1)
753296	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2177-1)
753330	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:2268-1)
753353	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP3) (SUSE-SU-2022:2262-1)
753486	SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 19 for SLE 15 SP3) (SUSE-SU-2022:2214-1)
902237	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9922)
902238	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9921)
902368	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9921-1)
902486	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9922-1)
907358	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9921-2)
940618	AlmaLinux Security Update for kernel (ALSA-2022:5249)
940638	AlmaLinux Security Update for kernel-rt (ALSA-2022:5267)

© [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](#)