



CVE-2022-21499

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

Summary

CVE	CVE-2022-21499
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-09 21:15:00 UTC
Updated	2022-09-28 20:00:00 UTC
Description	KGDB and KDB allow read and write access to kernel memory, and thus should be restricted during lockdown. An attacker

Risk And Classification

Problem Types: CWE-787

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	Oracle	Linux	6	-	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	8	-	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
Kernel Live Patch Security Notice LSN-0089-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
Debian -- Security Information -- DSA-5161-1 linux	DEBIAN	www.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

[159854](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9425)

159856 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9427)
159857 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9426)
159859 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9423)
159860 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9422)
159907 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-9495)
159910 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-9496)
160135 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9871)
160136 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9870)
160147 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9926)
160150 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9927)
160210 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)
160270 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)
179371 Debian Security Update for linux (DSA 5161-1)
184963 Debian Security Update for linux (CVE-2022-21499)
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)
240815 Red Hat Update for kernel-rt (RHSA-2022:7444)
240817 Red Hat Update for kernel security (RHSA-2022:7683)
240869 Red Hat Update for kernel-rt (RHSA-2022:7933)
240904 Red Hat Update for kernel security (RHSA-2022:8267)
242890 Red Hat Update for kernel (RHSA-2024:0724)
353993 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-016
353994 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-028
354007 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-015
354008 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-030

354017 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-032
354023 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-017
377117 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)
6140078 AWS Bottlerocket Security Update for kernel (GHSA-6xgh-x8jw-5xg6)
752231 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)
752234 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2080-1)
752240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2103-1)
752250 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2111-1)
752254 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2116-1)
752354 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2393-1)
752370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
753148 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)
753363 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 30 for SLE 15 SP1) (SUSE-SU-2022:2461-1)
753420 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 29 for SLE 15) (SUSE-SU-2022:2482-1)
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)
940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)
940766 AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)
940798 AlmaLinux Security Update for kernel (ALSA-2022:8267)
940843 AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)
960176 Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)
960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)

© [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](#).

