



# CVE-2022-21505

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

## Summary

<b>CVE</b>	CVE-2022-21505
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	Unknown
<b>Updated</b>	2021-11-15 20:11:31 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

## References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159988](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9612)

[159989](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9601)

[159990](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9602)

[159991](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9609)

[160043](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9709)

[160045](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9710)

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

[180939](#) Debian Security Update for linux (CVE-2022-21505)

[199295](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6031-1)

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

241468 Red Hat Update for kernel-rt (RHSA-2023:2148)
354049 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-034
354051 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-019
354055 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-007
354439 Amazon Linux Security Advisory for kernel : ALAS2022-2022-150
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)
6140350 AWS Bottlerocket Security Update for kernel (GHSA-cg53-fmp7-3g22)
752461 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2803-1)
752463 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2809-1)
752502 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2875-1)
753135 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2722-1)
753156 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2741-1)
753316 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2892-1)
941023 AlmaLinux Security Update for kernel (ALSA-2023:2458)
941061 AlmaLinux Security Update for kernel-rt (ALSA-2023:2148)

© [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](#)**