



# CVE-2021-4028

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

## Summary

<b>CVE</b>	CVE-2021-4028
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-24 16:15:00 UTC
<b>Updated</b>	2023-02-10 16:18:00 UTC
<b>Description</b>	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise</a>	15.0	sp3	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Linux Enterprise</a>	15.0	sp4	All	All

## References

Reference	Source
LKML: Greg Kroah-Hartman: [PATCH 5.10 22/93] RDMA/cma: Do not change route.addr.src_addr.ss_family	MISC
CVE-2021-4028 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFID
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
2027201 - (CVE-2021-4028) CVE-2021-4028 kernel: use-after-free in RDMA listen()	MISC
Bug 1193167 - VUL-0: CVE-2021-4028: kernel-source, kernel-source-rt, kernel-source-azure: kernel: use-after-free in RDMA listen()	MISC
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159740 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1198)
159766 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1550)
180126 Debian Security Update for linux (CVE-2021-4028)
240094 Red Hat Update for kpatch-patch (RHSA-2022:0590)
240100 Red Hat Update for kernel (RHSA-2022:0636)
240101 Red Hat Update for kernel-rt (RHSA-2022:0629)
240120 Red Hat Update for kpatch-patch (RHSA-2022:0772)
240121 Red Hat Update for kernel-rt (RHSA-2022:0771)
240122 Red Hat Update for kernel security (RHSA-2022:0777)
240195 Red Hat Update for kpatch-patch (RHSA-2022:1185)
240199 Red Hat Update for kernel security (RHSA-2022:1198)
240200 Red Hat Update for kernel-rt (RHSA-2022:1199)
240237 Red Hat Update for kpatch-patch (RHSA-2022:1535)
240243 Red Hat Update for kernel-rt (RHSA-2022:1555)
240249 Red Hat Update for kernel (RHSA-2022:1550)
240418 Red Hat Update for kpatch-patch (RHSA-2022:0851)
240440 Red Hat Update for kernel (RHSA-2022:1324)
753118 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP3) (SUSE-SU-2022:0295-1)
753292 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP3) (SUSE-SU-2022:0293-1)
753385 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 4 for SLE 15 SP3) (SUSE-SU-2022:0257-1)
753423 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP3) (SUSE-SU-2022:0270-1)
940484 AlmaLinux Security Update for kernel (ALSA-2022:1550)

© 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](#)**