



CVE-2021-3773

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

Summary

CVE	CVE-2021-3773
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-16 19:15:00 UTC
Updated	2023-02-24 14:41:00 UTC
Description	A flaw in netfilter could allow a network-connected attacker to infer openvpn connection endpoint information for further use

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	22.1.3	All	All	All
Application	Oracle	Communications Cloud Native Core Network Exposure Function	22.1.1	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	22.2.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source
2004949 – (CVE-2021-3773) CVE-2021-3773 kernel: lack of port sanity checking in natd and netfilter leads to exploit of OpenVPN clients	M
Oracle Critical Patch Update Advisory - July 2022	N
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159825](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)

[240275](#) Red Hat Update for kernel-rt (RHSA-2022:1975)

[240298](#) Red Hat Update for kernel security (RHSA-2022:1988)

[282256](#) Fedora Security Update for kernel (FEDORA-2022-b7ef5c55da)

[282260](#) Fedora Security Update for kernel (FEDORA-2022-a23dd56848)

[900667](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8676)

[902458](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10119)

[902516](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10117)

[940517](#) AlmaLinux Security Update for kernel (ALSA-2022:1988)

[960132](#) Rocky Linux Security Update for kernel-rt (RLSA-2022:1975)

[960134](#) Rocky Linux Security Update for kernel (RLSA-2022:1988)

© [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](#)