



CVE-2021-21781

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

Summary

CVE	CVE-2021-21781
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-18 15:15:00 UTC
Updated	2023-02-03 14:31:00 UTC
Description	An information disclosure vulnerability exists in the ARM SIGPAGE functionality of Linux Kernel v5.4.66 and v5.4.54. The la

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	5.4.54	All	All	All
Operating System	Linux	Linux Kernel	5.4.66	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

References

Reference	Source	Link	Tags
TALOS-2021-1243 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

178712 Debian Security Update for linux (DLA 2713-1)
178714 Debian Security Update for linux (DLA 2713-2)
179541 Debian Security Update for linux (CVE-2021-21781)
240298 Red Hat Update for kernel security (RHSA-2022:1988)
353097 Amazon Linux Security Advisory for kernel : ALAC2012-2021-033
353098 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-034
353099 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-035
610400 Google Pixel Android March 2022 Security Patch Missing
670707 EulerOS Security Update for kernel (EulerOS-SA-2021-2465)
671033 EulerOS Security Update for kernel (EulerOS-SA-2021-2569)
671181 EulerOS Security Update for kernel (EulerOS-SA-2021-2934)
671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)
750949 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1142-1)
750953 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2645-1)
750963 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2687-1)
940517 AlmaLinux Security Update for kernel (ALSA-2022:1988)
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](#)