



CVE-2022-2977

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-2977
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-14 21:15:00 UTC
Updated	2023-02-14 13:15:00 UTC
Description	A flaw was found in the Linux kernel implementation of proxied virtualized TPM devices. On a system where virtualized TPM

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
September 2022 Linux Kernel 5.17 Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 181057 Debian Security Update for linux (CVE-2022-2977)
- 672354 EulerOS Security Update for kernel (EulerOS-SA-2022-2732)
- 672391 EulerOS Security Update for kernel (EulerOS-SA-2022-2767)
- 672410 EulerOS Security Update for kernel (EulerOS-SA-2022-2796)

672454 EulerOS Security Update for kernel (EulerOS-SA-2022-2848)
672474 EulerOS Security Update for kernel (EulerOS-SA-2022-2823)
672711 EulerOS Security Update for kernel (EulerOS-SA-2023-1507)
752584 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3265-1)
752589 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3264-1)
752591 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3274-1)
752592 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3282-1)
752594 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3293-1)
752596 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3291-1)
752615 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3408-1)
752632 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3450-1)
753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)
753167 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3288-1)
753370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3609-1)
753374 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3809-1)
903916 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10946)
903917 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10967)
904092 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10946-1)
904253 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10967-1)
906116 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10946-2)
906345 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10967-2)

© [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](#)