



CVE-2024-26707

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

Summary

CVE	CVE-2024-26707
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-03 15:15:00 UTC
Updated	2024-04-03 17:24:00 UTC
Description	Description unavailable.

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

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/923dea2a7ea9e1ef5ac4031fba461c1cc92e32b8		git.kernel.org	
git.kernel.org/stable/c/56440799fc4621c279df16176f83a995d056023a		git.kernel.org	
git.kernel.org/stable/c/37e8c97e539015637cb920d3e6f1e404f707a06e		git.kernel.org	
git.kernel.org/stable/c/547545e50c913861219947ce490c68a1776b9b51		git.kernel.org	
git.kernel.org/stable/c/0d8011a878fdf96123bc0d6a12e2fe7ced5fddfb		git.kernel.org	
git.kernel.org/stable/c/de769423b2f053182a41317c4db5a927e90622a0		git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[6000567](#) Debian Security Update for linux (DSA 5658-1)

© 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](#)