



CVE-2024-26695

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

Summary

CVE	CVE-2024-26695
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/88aa493f393d2ee38ac140e1f6ac1881346e85d4		git.kernel.org	
git.kernel.org/stable/c/8731fe001a60581794ed9cf65da8cd304846a6fb		git.kernel.org	
git.kernel.org/stable/c/7535ec350a5f09b5756a7607f5582913f21200f4		git.kernel.org	
git.kernel.org/stable/c/58054faf3bd29cd0b949b77efcb6157f66f401ed		git.kernel.org	
git.kernel.org/stable/c/ccb88e9549e7cfd8bcd511c538f437e20026e983		git.kernel.org	
git.kernel.org/stable/c/b5909f197f3b26aebdca7d8ac7b688fd993a266		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