



SO_REUSEPORT_LB breaks connect(2) for UDP sockets

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

Summary

CVE	CVE-2025-24934
State	PUBLISHED
Assigner	freebsd
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-22 18:15:34 UTC
Updated	2026-04-24 00:16:26 UTC
Description	Software which sets SO_REUSEPORT_LB on a socket and then connects it to a host will not directly observe any problem

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from ADP

CVSS: 3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Problem Types: CWE-488 | CWE-488 CWE-488: Exposure of Data Element to Wrong Session

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	FreeBSD	FreeBSD	affected 15.0-BETA2 p1 beta	Not specified
CNA	FreeBSD	FreeBSD	affected 14.3-RELEASE p5 release	Not specified
CNA	FreeBSD	FreeBSD	affected 13.5-RELEASE p6 release	Not specified

References

Reference	Source	Link	Tags
security.freebsd.org/advisories/FreeBSD-SA-25:09.netinet.asc	secteam@freebsd.org	security.freebsd.org	
www.usenix.org/system/files/conference/usenixsecurity26/sec26_prepub_ben-sim...	secteam@freebsd.org	www.usenix.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

Vendor Comments And Credit

Discovery Credit

CNA: MSc. student Omer Ben Simhon from the Hebrew University School of Computer Science and Engineering (en)

CNA: Prof. Amit Klein from the Hebrew University School of Computer Science and Engineering (en)

There are currently no legacy QID mappings associated with this CVE.

© 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)