



# WebAssembly wabt binary-reader-interp.cc

## GetFuncOffset use after free

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

### Summary

<b>CVE</b>	CVE-2025-6275
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-06-19 20:15:24 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	A vulnerability was found in WebAssembly wabt up to 1.0.37. It has been declared as problematic. Affected by this vulnerat

### Risk And Classification

**Primary CVSS:** v4.0 1.9 LOW from cna@vulldb.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-119 | CWE-416 | CWE-416 Use After Free | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	4.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vulldb.com	Secondary	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	3.3	LOW	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	3.3	LOW	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	1.7		AV:L/AC:L/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	1.7		AV:L/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:ND/RC:UR

### CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webassembly	Wabt	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WebAssembly	Wabt	affected 1.0.0	Not specified
CNA	WebAssembly	Wabt	affected 1.0.1	Not specified
CNA	WebAssembly	Wabt	affected 1.0.2	Not specified
CNA	WebAssembly	Wabt	affected 1.0.3	Not specified
CNA	WebAssembly	Wabt	affected 1.0.4	Not specified
CNA	WebAssembly	Wabt	affected 1.0.5	Not specified
CNA	WebAssembly	Wabt	affected 1.0.6	Not specified
CNA	WebAssembly	Wabt	affected 1.0.7	Not specified
CNA	WebAssembly	Wabt	affected 1.0.8	Not specified
CNA	WebAssembly	Wabt	affected 1.0.9	Not specified
CNA	WebAssembly	Wabt	affected 1.0.10	Not specified
CNA	WebAssembly	Wabt	affected 1.0.11	Not specified
CNA	WebAssembly	Wabt	affected 1.0.12	Not specified
CNA	WebAssembly	Wabt	affected 1.0.13	Not specified
CNA	WebAssembly	Wabt	affected 1.0.14	Not specified
CNA	WebAssembly	Wabt	affected 1.0.15	Not specified

CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.16	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.17	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.18	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.19	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.20	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.21	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.22	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.23	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.24	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.25	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.26	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.27	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.28	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.29	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.30	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.31	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.32	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.33	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.34	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.35	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.36	Not specified
CNA	<a href="#">WebAssembly</a>	<a href="#">Wabt</a>	affected 1.0.37	Not specified

## References

Reference	Source	Link	Tags
<a href="https://github.com/user-attachments/files/20623626/wabt_crash_5.txt">github.com/user-attachments/files/20623626/wabt_crash_5.txt</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://github.com">github.com</a>	Exploit
<a href="https://github.com/WebAssembly/wabt/issues/2614">github.com/WebAssembly/wabt/issues/2614</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://github.com">github.com</a>	Exploit, Issue Tra
<a href="https://vuldb.com">vuldb.com</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Permissions Req
<a href="https://vuldb.com">vuldb.com</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
<a href="https://vuldb.com">vuldb.com</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advis
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analys

## Vendor Comments And Credit

Discovery Credit

**CNA:** JJLeo (VulDB User) (en)

### Additional Advisory Data

Source	Time	Event
CNA	2025-06-19T00:00:00.000Z	Advisory disclosed
CNA	2025-06-19T02:00:00.000Z	VulDB entry created
CNA	2025-06-19T08:44:03.000Z	VulDB entry last update

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](#)