WebAssembly Binaryen wasm-binary.cpp readExport heap-based overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-14956
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-19 17:15:51 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability was determined in WebAssembly Binaryen up to 125. Affected by this issue is the function WasmBinaryRea

Risk And Classification

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

CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-119 | CWE-122 | CWE-125 | CWE-122 Heap-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	1.9	LOW	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/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:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
3.1	cna@vuldb.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.3	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P
2.0	CNA	DECLARED	4.3		AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

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:L/VI:L/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/MSC: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

High

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WebAssembly	Binaryen	affected 125	Not specified

References

Reference	Source	Link	Tags
github.com/WebAssembly/binaryen	cna@vuldb.com	github.com	
vuldb.com	cna@vuldb.com	vuldb.com	Exploit, Third Party A
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advisory,
github.com/WebAssembly/binaryen/commit/4f52bff8c4075b5630422f902dd92a0af...	cna@vuldb.com	github.com	Patch
github.com/oneafter/1204/blob/main/hbf	cna@vuldb.com	github.com	Not Applicable
github.com/WebAssembly/binaryen/issues/8089	cna@vuldb.com	github.com	Exploit, Issue Trackir
github.com/WebAssembly/binaryen/pull/8092	cna@vuldb.com	github.com	Issue Tracking
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Require
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Vendor Comments And Credit

Discovery Credit

CNA: Oneafter (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-19T00:00:00.000Z	Advisory disclosed
CNA	2025-12-19T01:00:00.000Z	VulDB entry created
CNA	2025-12-30T20:37:02.000Z	VulDB entry last update

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