Wasmtime miscompiled guest heap access enables sandbox escape on aarch64 Cranelift

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

Summary

CVE	CVE-2026-34971
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 19:16:24 UTC
Updated	2026-04-13 21:16:25 UTC
Description	Wasmtime is a runtime for WebAssembly. From 32.0.0 to before 36.0.7, 42.0.2, and 43.0.1, Wasmtime's Cranelift compilati

Risk And Classification

Primary CVSS: v4.0 9 CRITICAL from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/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

EPSS: 0.000140000 probability, percentile 0.025400000 (date 2026-04-13)

Problem Types: CWE-125 | CWE-787 | CWE-125 CWE-125: Out-of-bounds Read | CWE-787 CWE-787: Out-of-bounds Write

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/V
4.0	CNA	DECLARED	9	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/V
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/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

High

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Bytecodealliance	Wasmtime	affected >= 32.0.0, < 36.0.7	Not specified
CNA	Bytecodealliance	Wasmtime	affected >= 37.0.0, < 42.0.2	Not specified

CNA	Bytecodealliance	Wasmtime	affected >= 43.0.0, < 44.0.1	Not specified

References

Reference	Source	Link	Tags
github.com/bytecodealliance/wasmtime/security/advisories/GHSA-jhxm-h53p-...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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