OpenClaw < 2026.3.31 - Compiler Binary Substitution via Environment Variable Override in Host Execution Policy

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

Summary

CVE	CVE-2026-41373
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 19:37:39 UTC
Updated	2026-05-01 15:46:57 UTC
Description	OpenClaw before 2026.3.31 contains an incomplete host-env-security-policy.json that fails to restrict compiler binary enviro

Risk And Classification

Primary CVSS: v4.0 5.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N/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: 0.000120000 probability, percentile 0.016800000 (date 2026-05-05)

Problem Types: CWE-427 | CWE-427 CWE-427 Uncontrolled Search Path Element

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	5.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openclaw	Openclaw	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenClaw	OpenClaw	affected 2026.3.31 semver	Not specified
CNA	OpenClaw	OpenClaw	unaffected 2026.3.31 semver	Not specified

References

Reference	Source	Link
github.com/openclaw/openclaw/commit/e277a37f896b5011a1df06e6490c6630074d...	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/openclaw-compiler-binary-substitution-via-environm...	disclosure@vulncheck.com	www.vulncheck.com
github.com/openclaw/openclaw/security/advisories/GHSA-g8xp-qx39-9jq9	disclosure@vulncheck.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: tdjackey (en)

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