



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

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

## Summary

<b>CVE</b>	CVE-2026-41373
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-28 19:37:39 UTC
<b>Updated</b>	2026-05-01 15:46:57 UTC
<b>Description</b>	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/MSX/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/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

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	<a href="#">OpenClaw</a>	<a href="#">OpenClaw</a>	affected 2026.3.31 semver	Not specified
CNA	<a href="#">OpenClaw</a>	<a href="#">OpenClaw</a>	unaffected 2026.3.31 semver	Not specified

References		
Reference	Source	Link
<a href="https://github.com/openclaw/openclaw/commit/e277a37f896b5011a1df06e6490c6630074d...">github.com/openclaw/openclaw/commit/e277a37f896b5011a1df06e6490c6630074d...</a>	disclosure@vulncheck.com	<a href="#">github.com</a>
<a href="https://www.vulncheck.com/advisories/openclaw-compiler-binary-substitution-via-environm...">www.vulncheck.com/advisories/openclaw-compiler-binary-substitution-via-environm...</a>	disclosure@vulncheck.com	<a href="#">www.vulncheck.com</a>
<a href="https://github.com/openclaw/openclaw/security/advisories/GHSA-g8xp-qx39-9jq9">github.com/openclaw/openclaw/security/advisories/GHSA-g8xp-qx39-9jq9</a>	disclosure@vulncheck.com	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

**Vendor Comments And Credit**

Discovery Credit

**CNA:** tdjackey (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](#)