



OpenClaw < 2026.3.31 - Environment Variable Override of Plugin Trust Root

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-41396 |
| State | PUBLISHED |
| Assigner | VulnCheck |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-28 19:37:43 UTC |
| Updated | 2026-04-28 20:10:23 UTC |
| Description | OpenClaw before 2026.3.31 allows workspace .env files to override the OPENCLAW_BUNDLED_PLUGINS_DIR environm |

Risk And Classification

Primary CVSS: v4.0 8.5 HIGH from disclosure@vulncheck.com

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

Problem Types: CWE-829 | CWE-829 CWE-829: Inclusion of Functionality from Untrusted Control Sphere

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------|-----------|-------|----------|---|
| 4.0 | disclosure@vulncheck.com | Secondary | 8.5 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA |
| 4.0 | CNA | CVSS | 8.5 | HIGH | CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA |
| 3.1 | disclosure@vulncheck.com | Primary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

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/330a9f98cb29c79b1c16a2117e03d6276a0d... | disclosure@vulncheck.com | github.com |
| www.vulncheck.com/advisories/openclaw-environment-variable-override-of-plugin-t... | disclosure@vulncheck.com | www.vulncheck.com |
| github.com/openclaw/openclaw/security/advisories/GHSA-qcj9-wwgw-6gm8 | 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: Nathan (@nexrin) (en)

CNA: KeenSecurityLab (en)

CNA: qclawer (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](#)