OpenClaw < 2026.4.20 - Arbitrary Code Execution via MCP stdio Environment Variables

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

Summary

CVE	CVE-2026-44995
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 18:16:39 UTC
Updated	2026-05-12 14:19:41 UTC
Description	OpenClaw before 2026.4.20 contains an improper environment variable validation vulnerability in MCP stdio server configu

Risk And Classification

Primary CVSS: v4.0 5.4 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

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

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	5.4	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.3	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

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:P/PR:L/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/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

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenClaw	OpenClaw	affected 2026.4.20 semver	Not specified
CNA	OpenClaw	OpenClaw	unaffected 2026.4.20 semver	Not specified

References

Reference	Source	Link
github.com/openclaw/openclaw/commit/62fa5071896e95edc7f67d1cebc70a2859e2...	disclosure@vulncheck.com	github.com
github.com/openclaw/openclaw/commit/85d86ebc4bf3d2226d39d132a484f4f7a299...	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/openclaw-arbitrary-code-execution-via-mcp-stdio-en...	disclosure@vulncheck.com	www.vulncheck.com
github.com/openclaw/openclaw/security/advisories/GHSA-mj59-h3q9-ghfh	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: Gus (@garagon) (en)

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