OpenClaw assertPublicHostname web-fetch.ts server-side request forgery

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

Summary

CVE	CVE-2026-6011
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-10 05:16:06 UTC
Updated	2026-04-30 14:22:11 UTC
Description	A weakness has been identified in OpenClaw up to 2026.1.26. Affected by this issue is some unknown functionality of the fi

Risk And Classification

Primary CVSS: v4.0 2.9 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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: 0.000450000 probability, percentile 0.137270000 (date 2026-04-15)

Problem Types: CWE-918 | CWE-918 Server-Side Request Forgery

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vuldb.com	Secondary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	5.6	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

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	Na	OpenClaw	affected 2026.1.0	Not specified
CNA	Na	OpenClaw	affected 2026.1.1	Not specified
CNA	Na	OpenClaw	affected 2026.1.2	Not specified
CNA	Na	OpenClaw	affected 2026.1.3	Not specified
CNA	Na	OpenClaw	affected 2026.1.4	Not specified
CNA	Na	OpenClaw	affected 2026.1.5	Not specified
CNA	Na	OpenClaw	affected 2026.1.6	Not specified
CNA	Na	OpenClaw	affected 2026.1.7	Not specified
CNA	Na	OpenClaw	affected 2026.1.8	Not specified
CNA	Na	OpenClaw	affected 2026.1.9	Not specified
CNA	Na	OpenClaw	affected 2026.1.10	Not specified
CNA	Na	OpenClaw	affected 2026.1.11	Not specified
CNA	Na	OpenClaw	affected 2026.1.12	Not specified
CNA	Na	OpenClaw	affected 2026.1.13	Not specified
CNA	Na	OpenClaw	affected 2026.1.14	Not specified

CNA	Na	OpenClaw	affected 2026.1.15	Not specified
CNA	Na	OpenClaw	affected 2026.1.16	Not specified
CNA	Na	OpenClaw	affected 2026.1.17	Not specified
CNA	Na	OpenClaw	affected 2026.1.18	Not specified
CNA	Na	OpenClaw	affected 2026.1.19	Not specified
CNA	Na	OpenClaw	affected 2026.1.20	Not specified
CNA	Na	OpenClaw	affected 2026.1.21	Not specified
CNA	Na	OpenClaw	affected 2026.1.22	Not specified
CNA	Na	OpenClaw	affected 2026.1.23	Not specified
CNA	Na	OpenClaw	affected 2026.1.24	Not specified
CNA	Na	OpenClaw	affected 2026.1.25	Not specified
CNA	Na	OpenClaw	affected 2026.1.26	Not specified
CNA	Na	OpenClaw	unaffected 2026.1.29	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/356567	cna@vuldb.com	vuldb.com	Third Party Adviso
github.com/openclaw/openclaw/commit/b623557a2ec7e271bda003eb3ac33fbb2e21...	cna@vuldb.com	github.com	Patch
github.com/openclaw/openclaw	cna@vuldb.com	github.com	Product
github.com/openclaw/openclaw/releases/tag/v2026.1.29	cna@vuldb.com	github.com	Release Notes
vuldb.com/submit/795224	cna@vuldb.com	vuldb.com	Patch, Third Party
vuldb.com/vuln/356567/cti	cna@vuldb.com	vuldb.com	Permissions Requ
github.com/zast-ai/vulnerability-reports/blob/main/openclaw/ssrf.md	cna@vuldb.com	github.com	Exploit, Mitigation,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: ZAST.AI (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-09T00:00:00.000Z	Advisory disclosed
CNA	2026-04-09T02:00:00.000Z	VulDB entry created
CNA	2026-04-09T16:34:14.000Z	VulDB entry last update

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**