



OpenClaw < 2026.3.25 - Brute-Force Attack via Missing Webhook Password Rate Limiting

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

Summary

CVE	CVE-2026-35623
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 22:16:30 UTC
Updated	2026-04-09 22:16:30 UTC
Description	OpenClaw before 2026.3.25 contains a missing rate limiting vulnerability in webhook authentication that allows attackers to

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from disclosure@vulncheck.com

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

Problem Types: CWE-307 | CWE-307 CWE-307 Improper Restriction of Excessive Authentication Attempts

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/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
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/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
3.1	disclosure@vulncheck.com	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.8	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

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: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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenClaw	OpenClaw	affected 2026.3.25 semver	Not specified
CNA	OpenClaw	OpenClaw	unaffected 2026.3.25 semver	Not specified

References

Reference	Source	Link
github.com/openclaw/openclaw/security/advisories/GHSA-xq8g-hgh6-87hv	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/openclaw-brute-force-attack-via-missing-webhook-pa...	disclosure@vulncheck.com	www.vulncheck.com
github.com/openclaw/openclaw/commit/5e08ce36d522a1c96df2bfe88e39303ae264...	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: Peng Zhou (@zpbrent) (en)

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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