



OpenClaw < 2026.3.28 - Brute Force Attack via Missing Rate Limiting on Webhook Shared Secret Authentication

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

Summary

CVE	CVE-2026-33580
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 15:16:15 UTC
Updated	2026-04-01 18:54:45 UTC
Description	OpenClaw before 2026.3.28 contains a missing rate limiting vulnerability in the Nextcloud Talk webhook authentication that

Risk And Classification

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

CVSS:4.0/AV:N/AC:L/AT:P/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

EPSS: 0.000570000 probability, percentile 0.178900000 (date 2026-04-01)

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:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	6.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	disclosure@vulncheck.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

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:L/AT:P/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

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/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	OpenClaw	OpenClaw	affected 2026.3.28 semver	Not specified		
CNA	OpenClaw	OpenClaw	unaffected 2026.3.28 semver	Not specified		
References						
Reference	Source	Link				
github.com/openclaw/openclaw/security/advisories/GHSA-9528-x887-j2fp	disclosure@vulncheck.com	github.com				
github.com/openclaw/openclaw/commit/e403decb6e20091b5402780a7ccd2085f98a...	disclosure@vulncheck.com	github.com				
www.vulncheck.com/advisories/openclaw-brute-force-attack-via-missing-rate-limit...	disclosure@vulncheck.com	www.vulncheck.com				
CVE Program record	CVE.ORG	www.cve.org				
NVD vulnerability detail	NVD	nvd.nist.gov				
Vendor Comments And Credit						
Discovery Credit						
CNA: AntAISecurityLab (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](#).

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