OpenClaw < 2026.3.31 - Fail-Open Security Scan Bypass in Plugin Installation

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

Summary

CVE	CVE-2026-41377
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 19:37:40 UTC
Updated	2026-05-01 15:50:40 UTC
Description	OpenClaw before 2026.3.31 contains a fail-open vulnerability in the plugin installation flow where security scan failures do r

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from disclosure@vulncheck.com

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

Problem Types: CWE-636 | CWE-636 CWE-636: Not Failing Securely (Failing Open)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA
3.1	disclosure@vulncheck.com	Primary	4.6	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	4.6	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/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 2026.3.31 semver	Not specified

CNA	OpenClaw	OpenClaw	unaffected 2026.3.31 semver	Not specified

References

Reference	Source	Link
www.vulncheck.com/advisories/openclaw-fail-open-security-scan-bypass-in-plugin-...	disclosure@vulncheck.com	www.vulncheck.com
github.com/openclaw/openclaw/commit/7a953a52271b9188a5fa830739a4366614ff...	disclosure@vulncheck.com	github.com
github.com/openclaw/openclaw/security/advisories/GHSA-cwq8-6f96-g3q4	disclosure@vulncheck.com	github.com
github.com/openclaw/openclaw/commit/bf96c67fd1954740aeabfadc7cfe3098bcfc...	disclosure@vulncheck.com	github.com
github.com/openclaw/openclaw/commit/0d7f1e2c84eca65df7dee890d9c30e2a841c...	disclosure@vulncheck.com	github.com
github.com/openclaw/openclaw/commit/44b993613601280d46a5b88190e46669fc13...	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: davidluzsilva (en)

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