



OpenClaw < 2026.3.8 - Script Content Modification via Mutable Operand Binding in system.run

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

Summary

CVE	CVE-2026-32921
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 12:16:28 UTC
Updated	2026-04-02 14:35:09 UTC
Description	OpenClaw before 2026.3.8 contains an approval bypass vulnerability in system.run where mutable script operands are not

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from disclosure@vulncheck.com

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

EPSS: 0.000480000 probability, percentile 0.149140000 (date 2026-04-01)

Problem Types: CWE-367 | CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/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:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/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:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	disclosure@vulncheck.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	CVSS	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

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 2026.3.8 semver	Not specified
CNA	OpenClaw	OpenClaw	unaffected 2026.3.8 semver	Not specified

References			
Reference	Source	Link	
github.com/openclaw/openclaw/commit/cf3a479bd1204f62eef7dd82b4aa328749ae...	disclosure@vulncheck.com	github.com	F
www.vulncheck.com/advisories/openclaw-script-content-modification-via-mutable-o...	disclosure@vulncheck.com	www.vulncheck.com	7
github.com/openclaw/openclaw/commit/c76d29208bf6a7f058d2cf582519d28069e4...	disclosure@vulncheck.com	github.com	F
github.com/openclaw/openclaw/security/advisories/GHSA-8g75-q649-6pv6	disclosure@vulncheck.com	github.com	V
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit
Discovery Credit
CNA: tdjackey (en)

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