



OpenClaw 2026.4.7 < 2026.4.10 - Sandbox Media Normalization Bypass via Discord Event Cover Image

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

Summary

| | |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| CVE | CVE-2026-43532 |
| State | PUBLISHED |
| Assigner | VulnCheck |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-05 12:16:19 UTC |
| Updated | 2026-05-05 19:32:49 UTC |
| Description | OpenClaw versions 2026.4.7 before 2026.4.10 fail to normalize Discord event cover image parameters in sandbox media p |

Risk And Classification

Primary CVSS: v4.0 4.9 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/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: 0.000370000 probability, percentile 0.109930000 (date 2026-05-05)

Problem Types: CWE-184 | CWE-184 CWE-184: Incomplete List of Disallowed Inputs

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------|-----------|-------|----------|---------------------------------------------------------------|
| 4.0 | disclosure@vulncheck.com | Secondary | 4.9 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA |
| 4.0 | CNA | CVSS | 4.9 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA |
| 3.1 | disclosure@vulncheck.com | Primary | 7.7 | HIGH | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N |
| 3.1 | CNA | CVSS | 7.7 | HIGH | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/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/MS:C: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

None

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------------------------|--------------------------|------------------------------------|---------------|
| CNA | OpenClaw | OpenClaw | affected 2026.4.7 2026.4.10 semver | Not specified |
| CNA | OpenClaw | OpenClaw | unaffected 2026.4.10 semver | Not specified |

References

References

| Reference | Source | Link |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------------------------------|
| www.vulncheck.com/advisories/openclaw-sandbox-media-normalization-bypass-via-di... | disclosure@vulncheck.com | www.vulncheck.com |
| github.com/openclaw/openclaw/security/advisories/GHSA-c9h3-5p7r-mrjh | disclosure@vulncheck.com | github.com |
| github.com/openclaw/openclaw/commit/979c6f09d6fad96596feb91c905934be7e0b... | 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: Akiyama Mio (@Telecaster2147) (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](#).

Free CVE JSON API cve.report/api

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