



OpenClaw < 2026.3.31 - Arbitrary Host File Read via appendLocalMediaParentRoots Self-Whitelisting

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-41366 |
| State | PUBLISHED |
| Assigner | VulnCheck |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-28 00:16:25 UTC |
| Updated | 2026-04-28 00:16:25 UTC |
| Description | OpenClaw before 2026.3.31 contains a local roots self-whitelisting vulnerability in appendLocalMediaParentRoots that allow |

Risk And Classification

Primary CVSS: v4.0 6 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/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-732 | CWE-732 CWE-732: Incorrect Permission Assignment for Critical Resource

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------|-----------|-------|----------|---|
| 4.0 | disclosure@vulncheck.com | Secondary | 6 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA |
| 4.0 | CNA | CVSS | 6 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA |
| 3.1 | disclosure@vulncheck.com | Primary | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| 3.1 | CNA | CVSS | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/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

High

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

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 |
|--|--------------------------|-------------------|
| github.com/openclaw/openclaw/security/advisories/GHSA-57gh-m6rq-54cf | disclosure@vulncheck.com | github.com |
| github.com/openclaw/openclaw/commit/1ca4261d7e055d0be141ed79ebb1365d0fbc... | disclosure@vulncheck.com | github.com |
| www.vulncheck.com/advisories/openclaw-arbitrary-host-file-read-via-appendlocalm... | 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: tdjackey (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