



# Crabbox < v0.12.0 Privilege Escalation via Agent Ticket Endpoints

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2026-8629  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | VulnCheck  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2026-05-14 20:17:21 UTC  |
| <b>Updated</b>         | 2026-05-15 14:11:05 UTC  |
| <b>Description</b>     | Crabbox prior to v0.12.0 contains a privilege escalation vulnerability that allows users with shared visibility-only access to o |

## Risk And Classification

**Primary CVSS:** v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/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:** 0.000210000 probability, percentile 0.060600000 (date 2026-05-18)

**Problem Types:** CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

| Version | Source                   | Type      | Score | Severity | Vector  |
|---------|--------------------------|-----------|-------|----------|---|
| 4.0     | disclosure@vulncheck.com | Secondary | 8.6   | HIGH     | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA |
| 4.0     | CNA                      | CVSS      | 8.6   | HIGH     | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA |
| 3.1     | disclosure@vulncheck.com | Primary   | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N                  |
| 3.1     | CNA                      | CVSS      | 8.1   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N                  |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

Unchanged

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

| Source | Vendor   | Product | Version   | Platforms     |
|--------|----------|---------|---|---------------|
| CNA    | Openclaw | Crabbox | affected 0.12.0 semver                                  | Not specified |
| CNA    | Openclaw | Crabbox | unaffected 95cb30dc7dbaa1fef690a42ef6ac1cb6e307a191 git | Not specified |

## References

| Reference  | Source                               | Link   |
|--|--------------------------------------|--|
| <a href="http://www.vulncheck.com/advisories/crabbox-privilege-escalation-via-agent-ticket-endp...">www.vulncheck.com/advisories/crabbox-privilege-escalation-via-agent-ticket-endp...</a> | disclosure@vulncheck.com             | <a href="http://www.vulncheck.com">www.vulncheck.com</a> |
| <a href="https://github.com/openclaw/crabbox/pull/71">github.com/openclaw/crabbox/pull/71</a>  | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | <a href="https://github.com">github.com</a>              |
| <a href="https://github.com/openclaw/crabbox/releases/tag/v0.12.0">github.com/openclaw/crabbox/releases/tag/v0.12.0</a>  | disclosure@vulncheck.com             | <a href="https://github.com">github.com</a>              |
| <a href="https://github.com/openclaw/crabbox/commit/95cb30dc7dbaa1fef690a42ef6ac1cb6e307a191">github.com/openclaw/crabbox/commit/95cb30dc7dbaa1fef690a42ef6ac1cb6e307a191</a>              | disclosure@vulncheck.com             | <a href="https://github.com">github.com</a>              |
| CVE Program record   | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>             |
| NVD vulnerability detail   | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>           |

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Chia Min Jun Lennon (en)

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)