



# OpenClaw < 2026.3.28 - SSRF Guard Bypass via IPv6 Special-Use Ranges

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

## Summary

<b>CVE</b>	CVE-2026-41361
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulnCheck
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-23 22:16:43 UTC
<b>Updated</b>	2026-04-23 22:16:43 UTC
<b>Description</b>	OpenClaw before 2026.3.28 contains an SSRF guard bypass vulnerability that fails to block four IPv6 special-use ranges. A

## Risk And Classification

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

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/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-184 | CWE-184 CWE-184: Incomplete List of Disallowed Inputs

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/SA
3.1	disclosure@vulncheck.com	Primary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality  
None

Integrity  
Low

Availability  
None

Sub Conf.  
High

Sub Integrity  
Low

Sub Availability  
None

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:L/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  
Changed

Confidentiality  
High

Integrity  
Low

Availability  
None

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



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	OpenClaw	OpenClaw	affected 2026.3.28 semver	Not specified
CNA	OpenClaw	OpenClaw	unaffected 2026.3.28 semver	Not specified

References

Reference	Source	Link
-----------	--------	------

www.vulncheck.com/advisories/openclaw-ssrf-guard-bypass-via-ipv6-special-use-ra...	disclosure@vulncheck.com	www.vulncheck.com
github.com/openclaw/openclaw/security/advisories/GHSA-g86v-f9qv-rh6m	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:** Nicky (@nicky-cc) of Tencent zhuque Lab (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](https://cve.report/api)

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