

Is 159.203.26.132 safe? TrustSniffer's low-trust assessment: 40/100

159.203.26.132

Verdict

40

OUT OF 100

LOW TRUST

159.203.26.132 is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Assessed 2026-08-18 by automated analysis. Classification confidence 55%.

What this site appears to be

A technical control UI for OpenClaw gateway with instructions to run a local gateway, obtain a tokenized dashboard URL, and paste a WebSocket URL and gateway token to connect. No visible forms or monetization elements.

Evidence status and limitations

Evidence completeness: UNKNOWN

- The real-world operator identity was not independently verified.
- Module-level completeness metadata is unavailable for this legacy report.

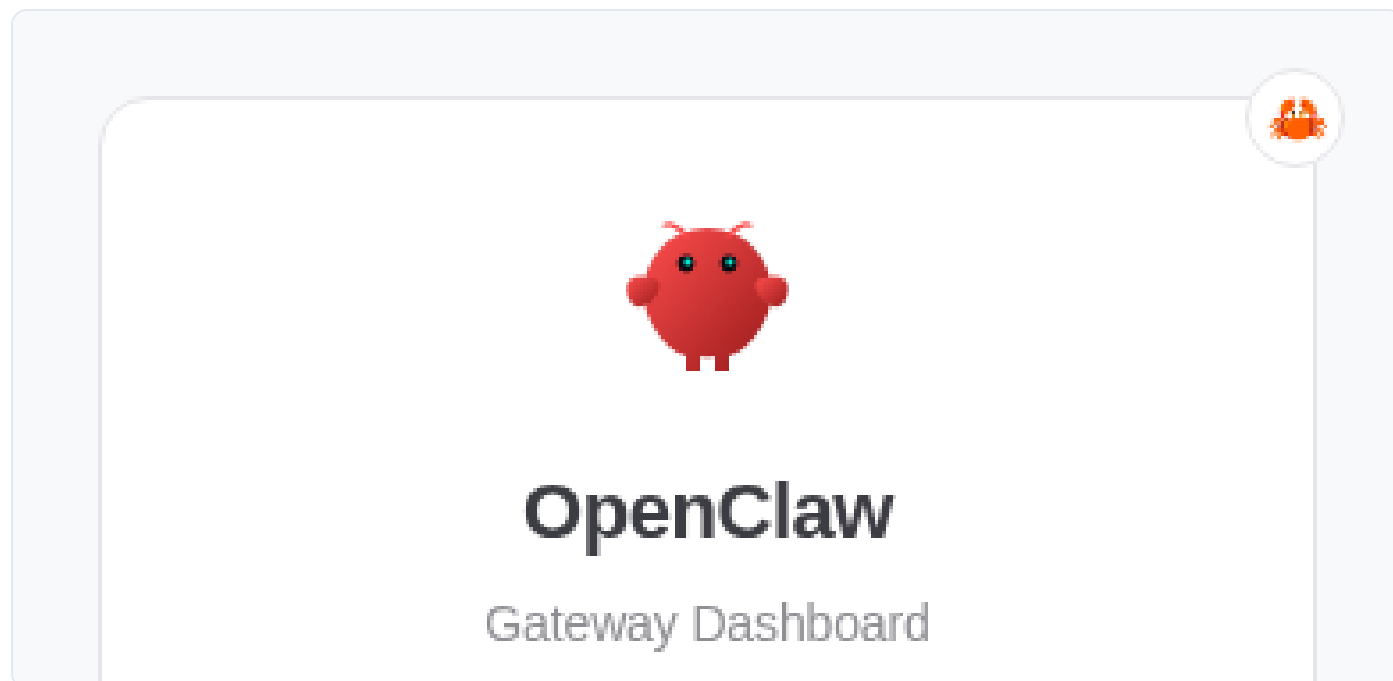
At a glance

The checks that decide most of this verdict.

Malware engines	4 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH

The page as captured

https://159.203.26.132/chat



What 159.203.26.132 served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Overview

The website is a technical control interface titled “OpenClaw Control,” presenting a gateway dashboard where visitors can enter a WebSocket URL and gateway token to connect to a locally running OpenClaw gateway; its apparent purpose is developer or systems-administration tooling rather than a commercial or financial service.

Scam/Impersonation Risk

The site’s visible content does not show brand impersonation, phishing forms, hidden forms, monetization, or other deceptive page features. However, the domain has a **confirmed blacklist status**, with four malicious detections recorded by external reputation checks; this is a material contradiction that outweighs the otherwise benign appearance of the control interface. The page also requests a gateway token and WebSocket connection details, creating a sensitive interaction surface even though the displayed interface states that the password is not stored. No conflicting legal identities were observed, and no suspicious contact-email anomaly was present.

EVIDENCE

- External reputation checks recorded 4 malicious detections and a confirmed blacklist status for the assessed address.
- The application dashboard displays fields for “WebSocket URL” and “Gateway Token,” together with a “Connect” control.
- The page analysis found no visible forms beyond the connection interface, no hidden forms, no wallet activity, and no external network requests during the observed interaction runs.

Regulatory Verification Notes

The available site content identifies the interface as OpenClaw Control but does not present an operator name, legal entity, licensing statement, registration number, or clearly accessible governance information. Because the service appears to be developer tooling rather than a regulated financial product, the absence of financial licensing language is not itself evidence of fraud; it remains a material identity and accountability gap for an enterprise deployment. The apparent legitimacy of the page’s technical purpose is therefore not sufficient to establish the real-world operator, particularly in light of the external blacklist finding.

EVIDENCE

- The captured page is titled “OpenClaw Control” and describes a local gateway/dashboard control function.
- The page provides a command to run a gateway locally and instructions to obtain a tokenized dashboard URL, but does not identify a responsible legal entity in the displayed content.
- The site is served from AS14061 (DigitalOcean, LLC), United States.

What to Verify Next

Before any sensitive interaction, the operator should obtain the software and documentation through an independently authenticated official channel and confirm that the assessed address is an authorized deployment. The gateway token and WebSocket endpoint should be supplied only after the endpoint, host ownership, and connection path have been validated by the responsible administrator. Any claimed organizational identity or regulatory status should be checked against the relevant corporate or sector registry rather than accepted from the site alone.

EVIDENCE

- The page instructs operators to start a local gateway and paste connection credentials into the dashboard.
- The page provides a “Read the docs” pathway but does not display independent operator or organizational verification.
- External reputation evidence conflicts with the page’s otherwise low-risk technical presentation and requires resolution before sensitive use.

Summary Verdict

The overall posture is **low trust with sensitive-interaction risk**. The site presents as a technically coherent utility, but its identity remains unverified and the confirmed external reputation contradiction prevents treating it as a reliable destination for credentials, authenticated access, or other sensitive activity.

Infrastructure Integrity

The website is protected by a CDN/WAF layer, and the observed address belongs to a CDN edge server rather than an independently observable origin. This reduces direct origin exposure and is a mitigating infrastructure characteristic, but it does not establish the legitimacy or safety of the service.

Closing Assessment

Enterprise users should restrict interaction to non-sensitive inspection until the deployment’s authorization, operator identity, and external reputation contradiction have been independently resolved.

Written analysis generated 2026-08-18 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine.

01 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.

Analysis engine signal:direct_threat

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of 159.203.26.132.

- The request stayed on 159.203.26.132. It was not redirected to another domain. [CLEAR](#)

Domain intelligence

Registrar	Not available
Hosting	Not available
Country	Not available
Server IP	159.203.26.132

Name servers	Not available
SSL issuer	Not available
SSL expiry	Not available
Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 4 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 159.203.26.132 at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/159.203.26.132> · assessed 2026-08-18