

Is luminexclient.net safe? TrustSniffer's low-trust assessment: 34/100

luminexclient.net

Verdict

34

OUT OF 100

LOW TRUST

luminexclient.net 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

Governance Risk

Assessed 2026-09-24 by automated analysis. Classification confidence 55%.

What this site appears to be

A software download page for Luminex Client, a Minecraft PvP-focused client (cheat/mod) offering a 26.2 Fabric build and a classic 1.21.11 build, feature list, installation instructions, and FAQ. No payment or account-login flows apparent.

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.

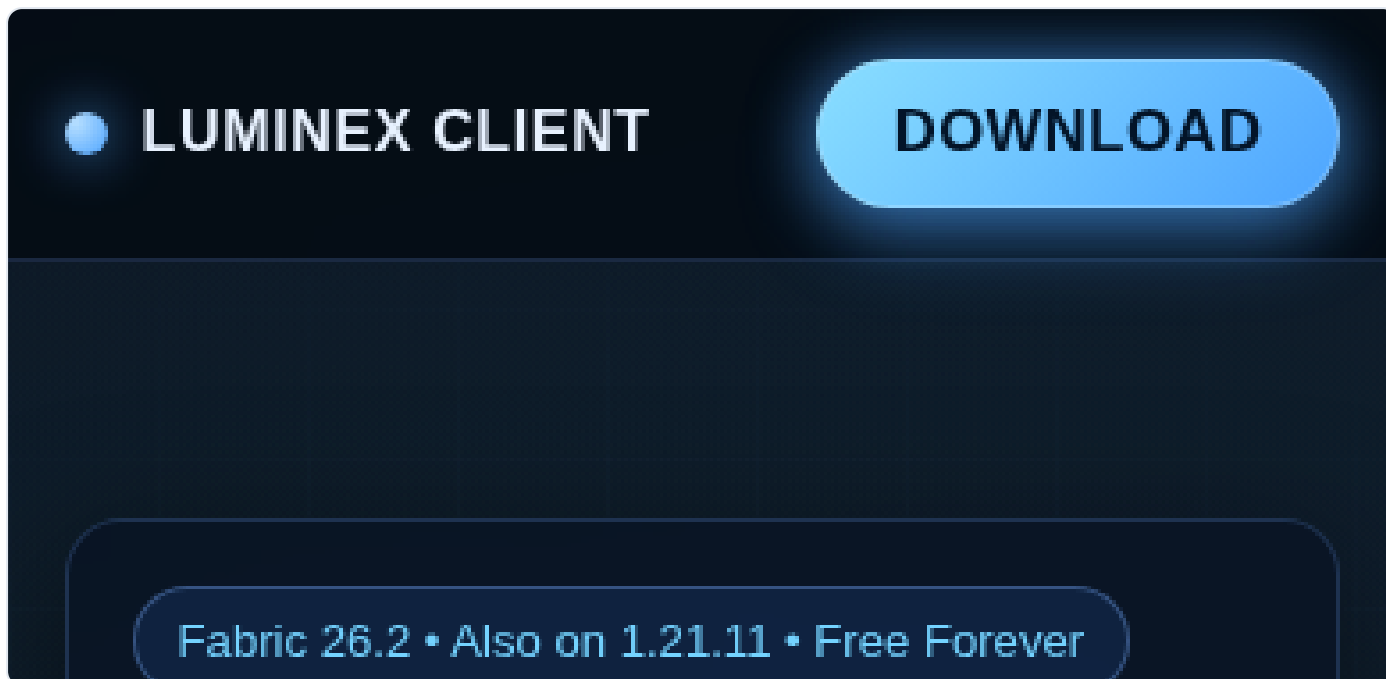
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	2 months old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://luminexclient.net/>



What luminexclient.net served when TrustSniffer captured it on 2026-09-24. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- No flags from the reputation services TrustSniffer consulted at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Security Alert

Fortinet flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

This website presents Luminex Client, a downloadable Minecraft PvP client/mod offered as a free software package for Fabric-based Minecraft installations. Its apparent purpose is to distribute a game modification featuring combat, movement, rendering, and utility modules, with installation instructions and direct download options rather than account, payment, or financial services.

Scam/Impersonation Risk

A confirmed blacklist hit creates a material contradiction and supports a clearly cautionary assessment. External security results also include two suspicious detections and a Fortinet threat detection, although the available page analysis did not identify brand impersonation, phishing forms, credential harvesting, payment flows, or deceptive redirects. The homepage nevertheless offers a directly downloadable executable mod, including modules such as Aim Assist, Trigger Bot, Auto Crystal, Player ESP, Freecam, and Self Destruct; this creates software-supply-chain and endpoint-safety exposure even though the page itself contains no explicit credential

or payment solicitation. No conflicting legal-entity names were observed, so the principal contradiction is the external blacklist and associated detections rather than an identity contradiction.

EVIDENCE

- External reputation telemetry records a confirmed blacklist hit for the domain; the same assessment records two suspicious detections and one Fortinet threat detection.
- The homepage offers direct downloads for Luminex Client builds and instructs users to place a `.jar`` file in the Minecraft mods folder.
- The homepage contains no login form, sensitive form, external password submission, or payment flow in the captured page.

Regulatory Verification Notes

The available site content does not establish a named legal operator, licensing authority, registration number, or independently verified real-world identity. This is a verification and disclosure gap rather than, by itself, proof of fraud; however, combined with the confirmed blacklist signal, it leaves the site's accountability and provenance unsuitable for sensitive interaction. The domain is very recently registered through Web Commerce Communications Limited dba WebNic.cc, which provides limited operating history for a site distributing executable software. No matching broker-reputation record was identified, but that absence is only contextual and does not offset the adverse external detection.

EVIDENCE

- Domain registration telemetry records creation on 2026-08-07T17:20:05Z, registration through Web Commerce Communications Limited dba WebNic.cc, and an age of 0.13 years.
- The homepage identifies the product as "Luminex Client" but does not provide a named corporate operator, licensing authority, or registration number in the captured content.
- The site's transport encryption uses a DV certificate issued by WE1, with validity recorded through 2026-11-08T06:50:03+00:00.

What to Verify Next

Before any interaction beyond passive inspection, an enterprise reviewer should obtain the operator's legal identity and independently confirm any applicable software distribution, consumer, or platform-policy requirements. The offered file should be checked for a verifiable publisher signature and hash, scanned with enterprise endpoint controls, and tested only in an isolated environment; installation should not occur on systems containing sensitive credentials or business data. Any support or contact channel should be confirmed through an independent route, and the adverse reputation status should be resolved with the relevant security or hosting stakeholders before deployment.

EVIDENCE

- The homepage provides installation instructions for Fabric Loader, Fabric API, and a downloadable `.jar`` file, making file provenance and integrity checks directly relevant.
- The captured page contains no visible publisher signature, file hash, corporate contact identity, or independent software-maintenance record.
- Behavioral observation recorded no external requests, hidden forms, wallet activity, clipboard manipulation, or cloaking during two successful runs; this limits the observed web-page behavior but does not validate the downloaded file.

Summary Verdict

The website has a **low-trust posture with elevated risk for sensitive interaction**. Its direct-download purpose and apparent lack of financial solicitation reduce the evidence of credential or payment fraud on the captured page, but they do not overcome the confirmed blacklist contradiction, limited identity assurance, and endpoint risk associated with executable distribution.

Infrastructure Integrity

The site is fronted by Cloudflare CDN/WAF infrastructure, and all observed addresses were CDN edge addresses rather than an exposed origin. This provides a meaningful layer of traffic and origin protection, but it is only a mitigating infrastructure characteristic and does not establish the legitimacy or safety of the site's downloadable software.

EVIDENCE

- Served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US).
- Observed edge address: 104.21.71.113; four CDN edge addresses were observed and zero likely origin candidates were identified.
- TLS certificate issued by WE1 (DV), valid to 2026-11-08T06:50:03+00:00.

Closing Assessment

The appropriate posture is to avoid downloading or executing the offered software until its publisher, file integrity, and adverse reputation status have been independently resolved; any required testing should remain isolated from sensitive systems and credentials.

Written analysis generated 2026-09-24 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by registration and ownership.

01 Governance Risk

- The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE

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 luminexclient.net.

- The request stayed on luminexclient.net. It was not redirected to another domain. CLEAR
- Registration is published under Web Commerce Communications Limited dba WebNic.cc. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-07. NOTED
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Web Commerce Communications Limited dba WebNic.cc
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3033::6815:4771
Name servers	ANDY.NS.CLOUDFLARE.COM, BRENNAN.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-11-08
Domain age	0.13 years (continuous registration)
Domain expiry	2027-08-07
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about luminexclient.net 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/luminexclient.net> · assessed 2026-09-24