

Is debugify.net a scam? TrustSniffer's high-risk assessment: 5/100

debugify.net

Verdict

5

OUT OF 100

CRITICAL RISK

debugify.net shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Debugify is a free, open-source Minecraft mod (Fabric 1.21.11) that consolidates 70+ bug fixes from the Mojang bug tracker into a single lightweight mod. The page provides features, installation steps, a full list of patched bug IDs, FAQ, license (LGPL-3.0), and download links.

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.

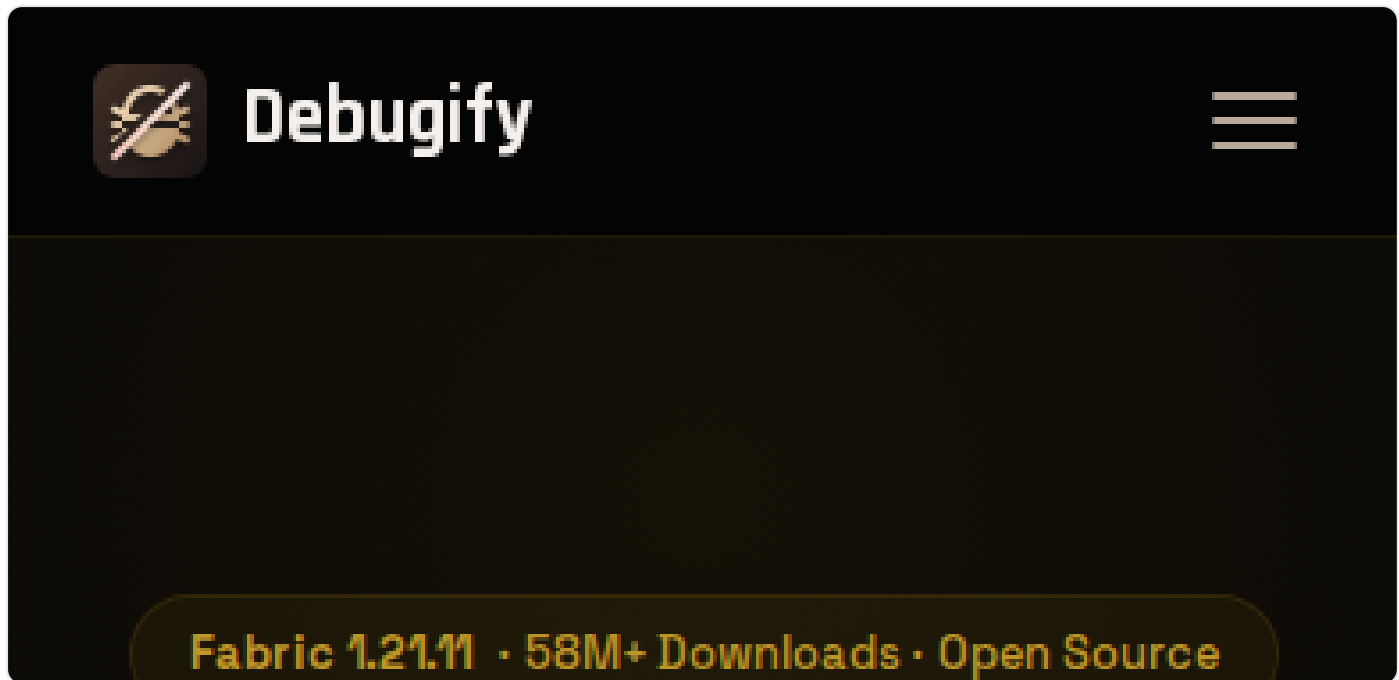
At a glance

The checks that decide most of this verdict.

Malware engines	3 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	4 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 YR1	NOTED

The page as captured

<https://debugify.net/>



What debugify.net served when TrustSniffer captured it on 2026-09-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- 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

Security Alert

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

This website presents Debugify as a free, open-source Minecraft mod for Fabric 1.21.11, offering a consolidated package of more than 70 bug fixes, installation guidance, configuration information, and direct download access; its apparent purpose is non-commercial software distribution rather than financial or subscription activity.

Scam/Impersonation Risk

The site's homepage presents a coherent software-project narrative, including bug-fix descriptions, installation instructions, patched Mojang bug identifiers, an FAQ, and an LGPL-3.0 license, with no observed login form, payment flow, or sensitive-data request. However, this benign presentation is outweighed by confirmed external blacklist status and multiple malicious or suspicious detections, including threat detections associated with Fortinet and Sophos. The site is therefore subject to a material reputation contradiction despite the absence of an observed brand-impersonation or identity-name conflict. The domain is also newly registered, which increases the importance of independently validating the download provenance before execution.

EVIDENCE

- The homepage describes Debugify as a Fabric 1.21.11 mod with more than 70 fixes, installation steps, an FAQ, and direct downloads.
- The homepage contains no observed login form, sensitive form, wallet interaction, or payment mechanism.
- External reputation assessment records a confirmed blacklist hit and multiple malicious or suspicious detections, including Fortinet and Sophos.
- Domain registration telemetry records creation on 2026-05-18 at 16:53:37 UTC, with an age of 0.35 years.

Regulatory Verification Notes

The available material supports a free software-project presentation rather than a regulated financial business model. The homepage identifies the project as open source and cites the LGPL-3.0 license, but the available pages do not independently establish the real-world operator or a legal entity responsible for distribution. Identity verification therefore remains incomplete, and the site should not be treated as an independently authenticated project merely because its content is detailed or technically coherent. No regulated-service licensing claim is established by the supplied evidence; this is a transparency and provenance matter rather than, by itself, proof of fraud.

EVIDENCE

- The homepage identifies the software as open source and presents an LGPL-3.0 license.
- The homepage provides project features, configuration guidance, and installation information but does not establish an independently verified legal operator.
- The observed business model is non-commercial software distribution, with no stated deposits, payments, or regulated financial service.

What to Verify Next

Before any executable download is opened, an independent official project source should be located and used to compare the publisher identity, release version, source code, and file hash or signature. The download should be tested in an isolated environment, and any claimed project ownership should be confirmed through an independently obtained contact or repository channel rather than relying solely on the website. If the site later requests an account, credentials, payment, or unrelated software installation, that request should be treated as inconsistent with the stated project purpose and independently validated before continuation.

EVIDENCE

- The homepage offers direct software downloads, making file provenance and integrity the principal immediate verification requirement.
- The homepage states that the project is open source and provides technical installation and configuration material that can be compared with an independent project source.
- The available evidence contains no observed account, payment, or sensitive-data workflow to explain or justify any such later request.

Summary Verdict

The overall posture is **critical trust risk**. The site’s polished and internally consistent software presentation does not overcome the confirmed blacklist and external threat-detection evidence, while the real-world operator remains unverified. Sensitive interaction with the site should therefore be regarded as unsuitable absent successful independent validation.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, and the observed address is an edge address rather than an independently exposed origin. This provides a mitigating layer against direct origin exposure but does not establish legitimacy, and edge-only visibility limits independent assessment of the underlying hosting environment.

EVIDENCE

- Observed edge infrastructure is associated with AS214351 and FEMOIT - FEMO IT SOLUTIONS LIMITED, GB.
- The observed edge address is 196.251.107.204; the infrastructure record identifies Cloudflare as the CDN/WAF provider and reports no observable origin candidate.
- TLS uses issuer YR1 with Domain Validation (DV), valid through 2026-12-20T14:07:47+00:00.

Closing Assessment

Prospective users should restrict activity to non-sensitive inspection until the project identity, download provenance, and file integrity have been independently confirmed; logins, credential submission, and financial interactions should not be undertaken.

Written analysis generated 2026-09-22 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, external reputation.

01 Governance Risk

- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

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 debugify.net.

- The request stayed on debugify.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 2027-05-18. NOTED
- It is hosted on FEMOIT, from a server in SC. NOTED

Domain intelligence

Registrar	Web Commerce Communications Limited dba WebNic.cc
Hosting	FEMOIT - FEMO IT SOLUTIONS LIMITED, GB
Country	SC
Server IP	196.251.107.204
Name servers	ANDY.NS.CLOUDFLARE.COM, BRENNAN.NS.CLOUDFLARE.COM
SSL issuer	YR1
SSL expiry	2026-12-20
Domain age	0.35 years (continuous registration)
Domain expiry	2027-05-18
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about debugify.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/debugify.net> · assessed 2026-09-22