Frothly

GL-AUDIT-2026

AUDIT REPORT

Glossia 4.0 Security Audit

An independent assessment of the protocol, reference clients and relay software.

Pauley & Finn Security

Glossia · Oct 2026

SUMMARY

Frothly engaged Pauley & Finn Security to audit Glossia 4.0 before its public release. Over nine weeks between July and September 2026, we reviewed the protocol specification, the reference clients for Android, iOS and desktop, and the relay software that carries messages between them.

We found no critical or high-severity issues. We reported three moderate and seven low-severity issues; all three moderate issues and five of the low-severity issues were fixed before release, and Frothly has documented its reasons for accepting the remaining two. In our assessment, Glossia 4.0 meets its published security goals.

KEY FINDINGS

01 The new hybrid post-quantum handshake was verified against its specification in a formal model, and its implementation matched the model in all tested cases.

02 No issue we found would allow an attacker to read message content, impersonate a user or recover past messages from a seized device.

03 Metadata exposure is lower than in Glossia 3.x. The two accepted issues concern timing and push notifications, and are documented for users who need the strongest protection.

04 Frothly's response to our findings was prompt and complete. All fixes were verified by us before release.

01

Scope

The audit covered version 4.0 of the Glossia protocol specification; the reference clients for Android, iOS and desktop at their release-candidate builds; and the relay server software used by Frothly and by community-operated relays. It did not cover third-party clients or the operational security of any particular relay operator.

Frothly provided full access to source code, design documents, the engineering team and previous audit reports. No part of the system was excluded at Frothly's request.

02

Method

- *Specification review.* A line-by-line review of the protocol specification, with particular attention to the new hybrid key exchange and to downgrade protection.
- *Formal verification.* We modeled the handshake in a symbolic protocol verifier and checked secrecy, authentication and forward secrecy properties under an active network attacker.
- *Code review.* Manual review of cryptographic code, key storage, attachment handling and relay message processing in all three clients and the relay.
- *Fuzzing.* 2.1 billion generated test cases against message parsers and the relay, using our fuzzing harness, Kuang.
- *Adversarial network testing.* Testing on simulated hostile networks, including high latency, packet loss, traffic shaping and active interference.

03

Results

0
Critical or high-severity issues

3
Moderate issues, all fixed before release

7
Low-severity issues: 5 fixed, 2 accepted

TABLE 1 Issues reported, by severity and status

Identifier	Severity	Issue	Status
GL4-M1	Moderate	Relays accepted malformed padding, allowing message sizes to be inferred	Fixed
GL4-M2	Moderate	Desktop client kept decrypted attachments in a temporary folder longer than necessary	Fixed
GL4-M3	Moderate	Key-transparency client did not pin the log's signing key on first use	Fixed
GL4-L1	Low	Verbose relay logging recorded connection times at full precision	Fixed
GL4-L2	Low	Android client allowed screenshots of the safety-number screen	Fixed
GL4-L3	Low	Session resumption tokens did not expire on device unlink	Fixed
GL4-L4	Low	Group invitations revealed member count before acceptance	Fixed
GL4-L5	Low	Specification ambiguity in the downgrade-protection section	Fixed
GL4-L6	Low	Delivery timing can reveal when a contact is online	Accepted
GL4-L7	Low	Push-notification providers learn when a device receives a message	Accepted

Severity follows our standard rating scale. Fixes were verified against release builds.

04

Moderate issues

GL4-M1: Padding inference at relays

Relays accepted messages whose padding did not conform to the specification. A malicious client could exploit this to send messages of distinctive sizes, allowing a network observer to correlate them. Relays now reject non-conforming padding.

GL4-M2: Decrypted attachments on desktop

The desktop client stored decrypted attachments in a temporary folder until the application closed. On a shared or seized computer, these files could be recovered. Attachments are now decrypted in memory and written to disk only when the user explicitly saves them.

GL4-M3: Key-transparency pinning

Clients verified the key-transparency log's signatures but did not pin the log's signing key on first use, so a client that first connected through a compromised network could be shown a forged log. Clients now ship with the signing key built in.

05

Accepted risks

Two low-severity issues were accepted by Frothly with documented reasoning, which we consider sound.

- *GL4-L6: Delivery timing.* When a message is delivered can reveal that a contact is online. Hiding this fully would require delaying every message. Glossia offers an optional random delay for users who need it.
- *GL4-L7: Push notifications.* Mobile push providers learn when a device receives a message, though not from whom. Glossia offers a mode that disables push notifications entirely, at some cost in battery life.

06

Conclusion

Glossia 4.0 is a careful, conservative design, and its implementation reflects that care. The hybrid handshake is a meaningful improvement for users whose messages must stay private for decades. We would be comfortable recommending it to the people it was built for.

This is the fourth independent audit of Glossia, following audits in 2014, 2018 and 2022. Previous reports remain available from Frothly.

References

Frothly (2026). *Glossia Protocol Specification, Version 4.0.* Chiba: Frothly.

Pauley & Finn Security (2022). *Glossia 3.0 Security Audit.* Report GL-AUDIT-2022.

Ravenor, G. (2016). Notes toward a private language. Frothly Working Paper FR-WP-2016-03.

About the authors

Pauley & Finn Security is an independent security consultancy. It has audited every major version of Glossia since 2014 and has no other commercial relationship with Frothly.

HOW TO CITE

Pauley & Finn Security (2026). *Glossia 4.0 Security Audit* An independent assessment of the protocol, reference clients and relay software. Frothly Audit report GL-AUDIT-2026. San Francisco: Frothly. https://frothly.org/programs/glossia/audit-2026/

Frothly

GL-AUDIT-2026

Frothly is an independent, not-for-profit research institute studying the systems that increasingly think, remember and decide on our behalf.

We hold no shares, sell no products and accept no funding that comes with conditions on our findings. Everything we publish is free to read.

San Francisco · Vancouver · Newark · Zürich · Chiba

This work is licensed under Creative Commons Attribution 4.0 International.