Fast withdrawal executor for Etherlink

Tezos Foundation

Independent security assessment report

inference

Report version: 1.0 / date: 07.07.2025

inference

Table of contents

Version / Date	Description
1.0 / 07.07.2025	Final version

inference

Summary

Inference AG was engaged by the Tezos Foundation to perform an independent security assessment of Etherlink's fast withdrawal executor. The fast withdrawal executor for Etherlink allows bridge operators to monitor an Etherlink L2 contract for withdrawal events and process them on the Tezos blockchain.

Inference AG performed the security assessment based on the agreed scope, following our approach and activities as outlined in the "Project overview" chapter between the 19th of May 2025 and the 17th of June 2025. Feedback from the Etherlink's fast withdrawal executor team was received and Inference performed a reassessment.

Based on our scope and our performed activities, our security assessment revealed a few security issues rated with a low severity. Additionally, different observations were also made. All of these were resolved with appropriate actions, improving the quality and security of the fast withdrawal executor.

This report highlights several risk-related points that bridge operators should consider when using the fast withdrawal executor.

Overview on findings

Details for each reported finding can be obtained from the "Findings" section.

Findings	Severity / Status
EWE-001: Private key management	Informational (for bridge operators)
EWE-002: Monitoring and potential loss of assets	Informational (for bridge operators)
EWE-003: Tezos and Etherlink RPC links	Informational (for bridge operators)

Project overview

Scope

The scope of the security assessment was the repository
https://github.com/etherlinkcom/fast-withdrawal-liquidity-executor

Our initial security assessment considered commit
“92e4bd687c946a1b43acc8662a40c385f91a7403”[1].

Our reassessment considered commit:
“a7baa9875d3231b02a97e188fb30bd00aaabeedb”[2].

Scope limitations

There are no specific limitations within the outlined scope.

[1] The sha256sum hash of the repository’s “.zip” file is:
595ec18c0489c8c7fbbfc98f76452e352dc071ff709d5efd31342cc1325723e3
[2] The sha256sum hash of the repository’s “.zip” file is:
48f99aee926df8d11032f0f463045a757b9910fe6a77b43249436804a8b41b98

Objectives

The objective is to perform an independent security assessment of the fast withdrawal executor for Etherlink. We reviewed the corresponding source code repository to evaluate whether it meets the following security requirements:

- Protects assets against loss due to technical issues
- Accurately identifies legitimate fast withdrawal transactions that meet defined parameters
- Rejects transactions with inadequate fees or amounts outside acceptable ranges
- Provides sufficient transparency to liquidity providers regarding the executor's status and funds
- Securely manages private keys
- Prevents execution of withdrawal transactions that might be reversed due to blockchain reorganization

Activities

Here is a list of general activities conducted during the security assessment for the previously defined scope:
Our security assessment activities for the defined scope were:

- Review of source code in the repository

Our activities for the reassessment were:

- Review of changes in the repository
- Reassessing security issues and observations from the initial assessment in case they are claimed to be resolved

Findings

EWE-001: Private key management

The current fast withdrawal executor provides three options for managing the private keys used to sign transactions when fronting tez to the bridge user: storing the private key in Amazon Secrets Manager, Google Secret Manager, or as an unencrypted parameter in the local environment file.

This poses a risk: if unauthorized individuals gain access to the machine hosting the fast withdrawal executor, or if the machine is compromised, the private key—and any assets it controls—could be stolen.

Recommendation
Bridge operators must be aware of this risk and implement appropriate safeguards, such as hardening the machine, enabling security monitoring, and limiting the amount of stored assets.

EWE-002: Monitoring and potential loss of assets

The current fast withdrawal executor does not

- Run the smart rollup in operator or accuser mode.

  This introduces the risk of asset loss if no honest smart rollup operator is active to refute incorrect commitments.

- Monitor and execute outbox messages if they are not processed by others.

  This creates a risk that, if no one executes the outbox messages, the bridge operator must do so themselves on time; otherwise, the assets locked in the smart rollup will remain inaccessible.

Recommendation
Bridge operators must be aware of this risk and, based on their specific risk profile and tolerance, define appropriate measures—such as verifying that at least one smart rollup operator is active, running the smart rollup in operator or accuser mode, monitoring the timely execution of outbox messages, and establishing procedures to manually execute outbox messages if they are not processed on time (e.g., running a smart rollup node in "executing_outbox" mode).

EWE-003: Tezos and Etherlink RPC links

The environment file allows setting the Tezos and Etherlink RPC endpoints using the variables TEZOS_RPC_URL and ETHERLINK_RPC, respectively. By default, these are configured to use local RPC nodes, which are launched alongside the fast withdrawal executor and provide finalized data from the Tezos or Etherlink blockchains.

However, bridge operators may be tempted to configure alternative RPC providers. Doing so introduces the risk of receiving inaccurate data—either due to a compromised machine or misconfiguration—which could ultimately result in the loss of assets.

Recommendation
Bridge operators should rely on the locally launched RPC endpoints provided by the fast withdrawal executor or, if using remote endpoints, ensure they are correctly configured and fully trusted. Additionally, operators should consider querying multiple RPC providers and comparing the results to verify consistency and reduce the risk of relying on a compromised or misconfigured system.

Disclaimer

This security assessment report ("Report") by Inference AG ("Inference") is solely intended for the Tezos Foundation ("Client") with respect to the Report's purpose as agreed by the Client. The Report may not be relied upon by any other party than the Client and may only be distributed to a third party or published with the Client's consent. If the Report is published or distributed by the Client or Inference (with the Client's approval) then it is for information purposes only and Inference does not accept or assume any responsibility or liability for any other purpose or to any other party.

Security assessments of a software or technology cannot uncover all existing vulnerabilities. Even an assessment in which no weaknesses are found is not a guarantee of a secure system. Generally, code assessments enable the discovery of vulnerabilities that were overlooked during development and show areas where additional security measures are necessary. Within the Client's defined time frame and engagement, Inference has performed an assessment in order to discover as many vulnerabilities of the technology or software analysed as possible. The focus of the Report's security assessment was limited to the general items and code parts defined by the Client. The assessment shall reduce risks for the Client but in no way claims any guarantee of security or functionality of the technology or software that Inference agreed to assess. As a result, the Report does not provide any warranty or guarantee regarding the defect-free or vulnerability-free nature of the technology or software analysed.

In addition, the Report only addresses the issues of the system and software at the time the Report was produced. The Client should be aware that blockchain technology and cryptographic assets present a high level of ongoing risk. Given the fact that inherent limitations, errors or failures in any software development process and software product exist, it is possible that even major failures or malfunctions remain undetected by the Report. Inference did not assess the underlying third party infrastructure which adds further risks. Inference relied on the correct performance and execution of the included third party technology itself.

Appendix

Risk rating definition

Severity definition is based on the OWASP Risk Rating Methodology and NIST SP800-30. It implements a categorization mechanism to divide findings into four different categories, presented here along with their definitions.

High

Risks classified as High are severe and immediate threats to your system's security and operations. These risks often have a high likelihood of occurrence and could lead to significant, potentially catastrophic, consequences affecting confidentiality, integrity, or availability. High risks require urgent attention and swift action to mitigate or remediate. They typically involve vulnerabilities that are easy to exploit and have a significant impact, such as those leading to data loss, financial damage, legal repercussions, or severe reputational harm.

Medium

Medium risks are significant concerns that pose a considerable threat to system security or data integrity but are less urgent than high risks. They might have a moderate likelihood of occurrence or impact, requiring attention and appropriate measures to mitigate. Medium risks might include vulnerabilities that are less likely to be exploited or have less severe impacts but still warrant timely intervention to prevent escalation or exploitation.

Low

Low risks are vulnerabilities or threats with minimal impact and likelihood of occurrence. They represent minor issues that do not significantly affect the system's overall security posture. While they require attention and should be addressed to maintain a robust security stance, they do not pose immediate or substantial threats.

Informational

Informational entries are not risks per se. They are included to suggest potential areas for improvement, or note deviations from best practices. These findings are typically items that do not have a direct or immediate impact on security but may influence security posture over time. They are valuable for comprehensive understanding, future planning, or awareness.

Glossary

Term	Description
Bridge	Solution to transfer tokens from a chain or a layer to a different chain or layer
Etherlink	Smart optimistic rollup