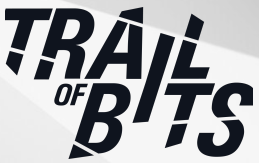

Offchain Geth 14.4 Changes for Pectra

Security Assessment (Summary Report)

March 12, 2025

Prepared for:
Harry Kalodner, Lee Bousfield, Steven Goldfeder, and Ed Felten
Offchain Labs

Prepared by: **Gustavo Grieco**

Table of Contents

Project Summary

Contact Information

The following project manager was associated with this project:

Mary O'Brien, Project Manager
mary.obrien@trailofbits.com

The following engineering director was associated with this project:

Josselin Feist, Engineering Director, Blockchain
josselin.feist@trailofbits.com

The following consultant was associated with this project:

Gustavo Grieco, Consultant
gustavo.grieco@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
February 10, 2025	Delivery of report draft
February 14, 2025	Report readout meeting
March 12, 2025	Delivery of final summary report

Executive Summary

Engagement Overview

Offchain Labs engaged Trail of Bits to review the security of the changes adding support for Geth 14.4 for the go-ethereum fork used in ArbOS. These changes correspond to revisions made in `53f5c56` (Nitro) and `b6f989a` (go-ethereum).

The commits in scope involve a number of upstream changes related to Geth 14.4 support as well as Arbitrum-specific changes, including support for preimage recording, cache and database improvements, and other minor changes. Only potential consensus-related changes were in scope. These were determined by the two diff files provided by Offchain Labs showing changes impacting the replay executable: one by line intersections and one by hunk intersections.

One consultant conducted the review from February 5 to February 10, 2025, for a total of four engineer-days of effort. With full access to source code and documentation, we performed a manual review of the code in scope.

Observations and Impact

This engagement did not reveal any issues in the code in scope. However, we provide some recommendations for improving the code quality in the Code Quality Recommendations appendix.

Recommendations

Based on the security review, Trail of Bits recommends that Offchain Labs take the following step:

- Review the items in the Code Quality Recommendations appendix and consider taking action on each one.

A. Code Quality Recommendations

The following is a list of findings that were not identified as immediate security issues but may warrant further investigation.

- Consider adding additional documentation on changes that could affect consensus. While a number of the upstream Geth 14.4 changes should not affect consensus, these changes were tested only on the Ethereum mainnet, without considering Arbitrum-specific assumptions. In particular, from the `state_transition` changes in scope, the following changes need to be documented:
    - The coinbase/tip address was changed since the tip is always zero.
    - The `msg.value` balance addition was moved outside the `st.msg.GasFeeCap != nil` check (e.g., make sure that the `else` branch is never used).

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 100+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at https://github.com/trailofbits/publications, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow @trailofbits on Twitter and explore our public repositories at https://github.com/trailofbits. To engage us directly, visit our "Contact" page at https://www.trailofbits.com/contact, or email us at info@trailofbits.com.

Trail of Bits, Inc.
228 Park Ave S #80688
New York, NY 10003
https://www.trailofbits.com
info@trailofbits.com

Notices and Remarks

Copyright and Distribution

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Trail of Bits uses automated testing techniques to rapidly test the controls and security properties of software. These techniques augment our manual security review work, but each has its limitations: for example, a tool may not generate a random edge case that violates a property or may not fully complete its analysis during the allotted time. Their use is also limited by the time and resource constraints of a project.