Gensyn ERC-20 Token

Security Assessment (Summary Report)

September 26, 2025

Prepared for:
Harry Grieve
Gensyn

Prepared by: **Simone Monica**

Table of Contents

Table of Contents 1
Project Summary 2
Project Targets 3
Executive Summary 4
About Trail of Bits 5
Notices and Remarks 6

Project Summary

Contact Information

The following project manager was associated with this project:

Kimberly Espinoza, Project Manager
kimberly.espinoza@trailofbits.com

The following engineering director was associated with this project:

Benjamin Samuels, Engineering Director, Blockchain
benjamin.samuels@trailofbits.com

The following consultant was associated with this project:

Simone Monica, Consultant
simone.monica@trailofbits.com

Project Timeline

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

Date	Event
September 19, 2025	Pre-project kickoff call
September 22, 2025	Delivery of report draft
September 26, 2025	Delivery of final summary report

Project Targets

The engagement involved reviewing and testing the following target.

Gensyn Token

Repository	https://github.com/gensyn-ai/gensyn-token
Version	`433abeb0998f59e54b0cf800d5825470c3eb361d`
Type	Solidity
Platform	Gensyn

Executive Summary

Engagement Overview

Gensyn engaged Trail of Bits to review the security of its ERC-20 token, which is built on the OpenZeppelin contracts. It is burnable, is upgradeable, supports EIP-2612, and can be used to vote on a governance system.

One consultant conducted the review on September 22, 2025, for a total of one engineer-day of effort. With full access to source code and documentation, we performed static testing of the codebase, using automated and manual processes.

Observations and Impact

We assessed whether the Gensyn token correctly uses the OpenZeppelin contracts and whether appropriate access controls are in place for permissioned actions, such as upgrading to a new contract implementation.

We also reviewed the deployment script to determine if the token's configuration matches its documentation. In particular, we assessed whether the upgrade has a delay of seven days since being proposed. Additionally, we checked for ways to mint tokens outside of the initial mint when initialized.

Overall, we found no issues.

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 assessments, supporting client organizations in the technology, defense, blockchain, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, Uniswap, Solana, Ethereum Foundation, Linux Foundation, and Zoom.

To keep up with our latest news and announcements, please follow @trailofbits on X or LinkedIn 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

Trail of Bits performed all activities associated with this project in accordance with a statement of work and an agreed-upon project plan.

Security assessment projects are time-boxed and often rely on information 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 software controls and security properties. 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. A project's time and resource constraints also limit their use.