Sec3™

Security Assessment Report

# Marginfi v2 Emode

June 30, 2025

# Summary

The Sec3 team (formerly Soteria) was engaged to conduct a thorough security analysis of the Marginfi v2 Emode feature.

The artifact of the audit was the source code of the following programs, excluding tests, in PR#318 and PR#335.

The initial audit focused on the following versions and revealed 1 issues or questions.

| # | program | type | commit |
|---|---|---|---|
| P1 | Marginfi v2 PR#318 | Solana | 82146661391f52ee7c55a9bcdc9f5d3ee811d71c |
| P2 | Marginfi v2 PR#335 | Solana | 9351e0b4d4a5e150d7172d0ab3c7eb6a03657f4e |

This report provides a detailed description of the findings and their respective resolutions.

# Table of Contents

# Result Overview

| Issue | Impact | Status |
|---|---|---|
| **MARGINFI V2 PR#318** | | |
| [P1-I-01] Missing excessive maintenance weights check in StakedSettings | Info | Resolved |
| **MARGINFI V2 PR#335** | | |
| No issues found | | |

# Findings in Detail

### MARGINFI V2 PR#318

## [P1-I-01] Missing excessive maintenance weights check in StakedSettings

This pull request introduces a new check for excessive maintenance weights, enforcing a cap of 200% to prevent accidental misconfiguration.

```
/* programs/marginfi/src/state/marginfi_group.rs */
check!(
    asset_maint_w <= (I80F48::ONE + I80F48::ONE),
    MarginfiError::InvalidConfig
);
```

However, this check has only been applied to `EmodeSettings` and `BankConfig`. It is recommended to also port this check to `StakedSettings`, where the same validation logic should theoretically apply.

### Resolution

This issue has been fixed by `3e418b1`.

# Appendix: Methodology and Scope of Work

Assisted by the Sec3 Scanner developed in-house, the manual audit particularly focused on the following work items:

- Check common security issues.
- Check program logic implementation against available design specifications.
- Check poor coding practices and unsafe behavior.
- The soundness of the economics design and algorithm is out of scope of this work

# DISCLAIMER

The instance report ("Report") was prepared pursuant to an agreement between Coderrect Inc. d/b/a Sec3 (the "Company") and MRGN, Inc. (the "Client''). This Report solely includes the results of a technical assessment of a specific build and/or version of the Client's code specified in the Report ("Assessed Code") by the Company. The sole purpose of the Report is to provide the Client with the results of the technical assessment of the Assessed Code. The Report does not apply to any other version and/or build of the Assessed Code. Regardless of the contents of the Report, the Report does not (and should not be interpreted to) provide any warranty, representation or covenant that the Assessed Code: (i) is error and/or bug free, (ii) has no security vulnerabilities, and/or (iii) does not infringe any third-party rights. Moreover, the Report is not, and should not be considered, an endorsement by the Company of the Assessed Code and/or of the Client. Finally, the Report should not be considered investment advice or a recommendation to invest in the Assessed Code and/or the Client.

This Report is considered null and void if the Report (or any portion thereof) is altered in any manner.

# ABOUT

The Sec3 audit team comprises a group of computer science professors, researchers, and industry veterans with extensive experience in smart contract security, program analysis, testing, and formal verification. We are also building automated security tools that incorporate static analysis, penetration testing, and formal verification.

At Sec3, we identify and eliminate security vulnerabilities through the most rigorous process and aided by the most advanced analysis tools.

For more information, check out our website and follow us on twitter.

Sec3™