// HALBORN

DeBridge - Solana Contracts

Solana Program Security Audit

Prepared by: **Halborn**

Date of Engagement: **November 28th, 2022 - December 16th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	11/29/2022	Michael Smith
0.2	Final Draft	12/15/2022	Michael Smith
0.3	Draft Review	12/16/2022	Isabel Burruezo
0.4	Draft Review	12/16/2022	Piotr Cielas
0.5	Draft Review	12/16/2022	Gabi Urrutia
1.0	Remediation Plan	01/12/2023	Michael Smith
1.1	Remediation Plan Review	01/12/2023	Isabel Burruezo
1.2	Remediation Plan Review	01/12/2023	Piotr Cielas
1.3	Remediation Plan Review	01/12/2023	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Piotr Cielas	Halborn	Piotr.Cielas@halborn.com
Isabel Burruezo	Halborn	Isabel.Burruezo@halborn.com
Michael Smith	Halborn	Michael.Smith@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

deBridge is a cross-chain interoperability and liquidity transfer protocol that allows decentralized transfer of assets between various blockchains. The cross-chain intercommunication of deBridge programs is powered by the network of independent oracles/validators which are elected by deBridge governance.

DeBridge engaged Halborn to conduct a security audit on their Solana programs beginning on November 28th, 2022 and ending on December 16th, 2022 . The security assessment was scoped to the programs provided in the Solana Contracts GitHub repository. Commit hashes and further details can be found in the Scope section of this report.

1.2 AUDIT SUMMARY

The team at Halborn was provided 3 weeks for the engagement and assigned a full-time security engineer to audit the security of the programs in scope. The security engineer is a blockchain and smart contract security expert with advanced penetration testing and smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of this audit is to:

- Identify potential security issues within the programs

In summary, Halborn identified some improvements to reduce the likelihood and impact of multiple risks, which has been successfully addressed by DeBridge . The main ones are the following:

- Fees can negate the send amount.

DeBridge acknowledged this finding and confirmed that this is a feature and that this is expected behavior.

1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of a manual review of the source code and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of the program audit. While manual testing is recommended to uncover flaws in business logic, processes, and implementation; automated testing techniques help enhance coverage of programs and can quickly identify items that do not follow security best practices.

The following phases and associated tools were used throughout the term of the audit:

- Research into the architecture, purpose, and use of the platform.
- Manual program source code review to identify business logic issues.
- Mapping out possible attack vectors
- Thorough assessment of safety and usage of critical Rust variables and functions in scope that could lead to arithmetic vulnerabilities.
- Finding unsafe Rust code usage (cargo-geiger)
- Scanning dependencies for known vulnerabilities (cargo audit).
- Local runtime testing (solana-test-framework)

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.
3 - Potential of a security incident in the long term.
2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

10 - CRITICAL
9 - 8 - HIGH
7 - 6 - MEDIUM
5 - 4 - LOW
3 - 1 - VERY LOW AND INFORMATIONAL

1.4 SCOPE

Code repositories:

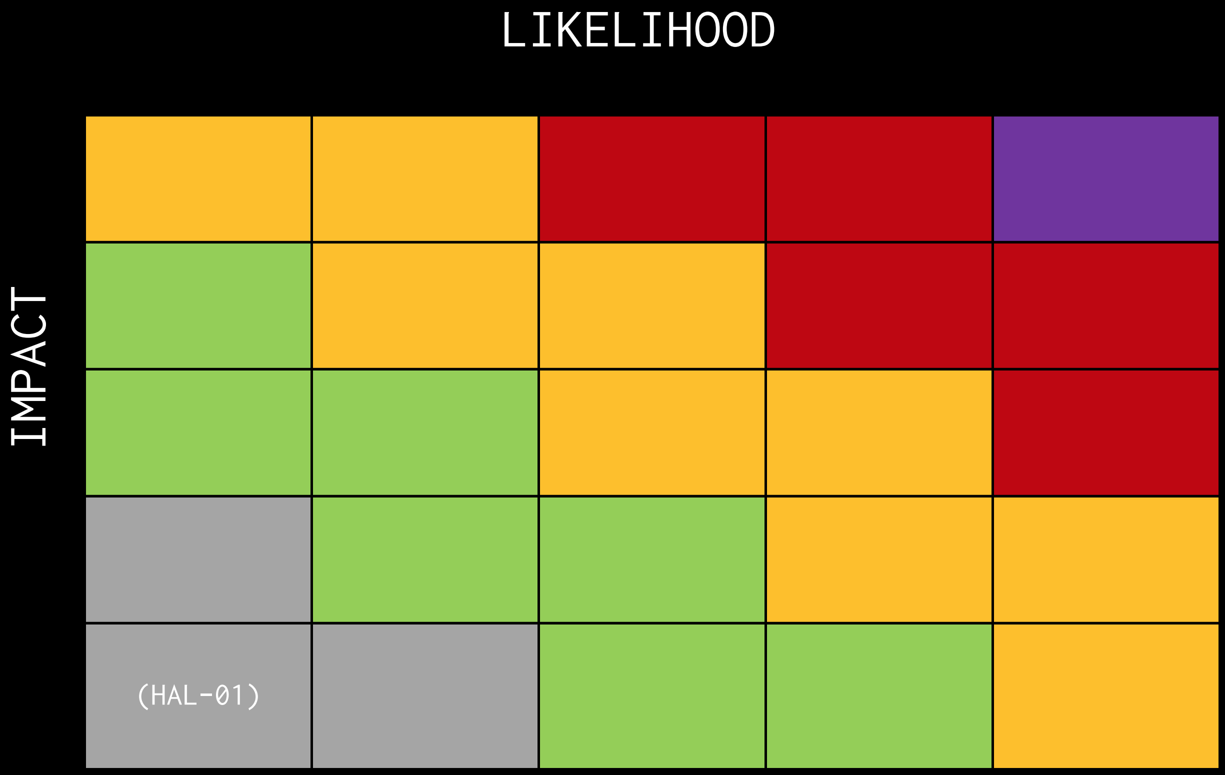
1. Project Name

- Repository: Solana Contracts
- Commit ID: d9fba17ee028db017af601dccf33e82c48a8b251
- Programs in scope:
    1. Debride (programs/debridge)
    2. Debride Settings (programs/settings)

Out-of-scope:
- third-party libraries and dependencies
- financial-related attacks

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	0	0	0	1



SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
HAL-01 - FEES CAN NEGATE SEND AMOUNT	Informational	ACKNOWLEDGED

FINDINGS & TECH DETAILS

3.1 (HAL-01) FEES CAN NEGATE SEND AMOUNT - INFORMATIONAL

Description:

The Debridge programs allows users to send tokens to other chains with the send instruction. The fix_fee, transfer_fee and execution_fee charged to the user can be equivalent to the original amount of tokens sent, resulting in the final_amount of tokens the user receives on the other chain to be zero.

Code Location:

Listing 1: programs/debridge/src/lib.rs (Lines 120,129,133,138)

```
84  pub fn send(
85      ctx: Context<Sending>,
86      target_chain_id: [u8; 32],
87      receiver: Vec<u8>,
88      is_use_asset_fee: bool,
89      amount: u64,
90      submission_params: Option<SendSubmissionParamsInput>,
91      referral_code: Option<u32>,
92  ) -> Result<()> {
93      let mut transfer_builder = Box::new(events::TransferredBuilder
    ↳ ::default());
94      transfer_builder.referral_code(referral_code);
95
96      {
97          let chain_address_len = ctx
98              .accounts
99              .bridge_ctx
100             .chain_support_info
101             .get_chain_address_len(&target_chain_id)?;
102         require!(
103             receiver.len().eq(&chain_address_len),
104             DebridgeErrorCode::WrongReceiverAddress,
105         );
106         require!(
107             submission_params
```

```rust
                .as_ref()
                .map(|param| param.fallback_address.len().eq(&chain_address_len))
                .unwrap_or(true),
            DebridgeErrorCode::WrongFallbackAddress,
        );
    }

    let fee_type = FeeType::new(is_use_asset_fee);
    let send_fix_fee = Box::new(ctx.accounts.get_fix_fee_sender(fee_type));
    let send_transfer_fee = Box::new(ctx.accounts.get_transfer_fee_sender());
    let process_exectuion_fee = Box::new(ctx.accounts.get_bridge_balance_changer());

    let final_amount = ctx
        .accounts
        .get_amount_context(
            ctx.accounts.send_token(amount)?,
            submission_params
                .as_ref()
                .map(|params| params.execution_fee),
            &target_chain_id,
        )?
        .take_fix_fee(send_fix_fee.add_pre_process(|fee| {
            transfer_builder.collected_fee(fee);
            Ok(())
        }))?
        .take_transfer_fee(|transfer_fee| {
            transfer_builder.collected_transfer_fee(transfer_fee);
            send_transfer_fee(transfer_fee)
        })?
        .process_amount_at_bridge(process_exectuion_fee)?
        .take_execution_fee(|execution_fee| {
            transfer_builder.execution_fee(execution_fee);
        })
        .amount();
```

Recommendation:

Validate that the final amount of tokens sent is not zero, if it is the transaction should fail.

Remediation Plan:

ACKNOWLEDGED: The Debridge team acknowledged this finding.

MANUAL TESTING

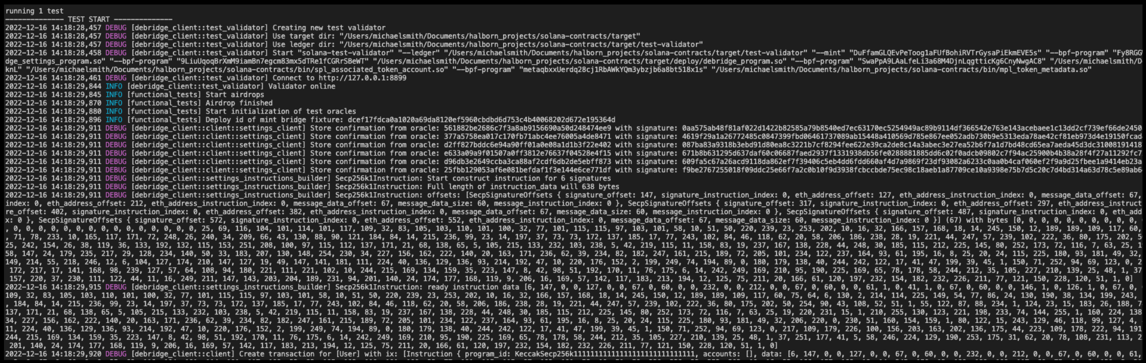
In the manual testing phase, the following scenarios were simulated. The scenarios listed below were selected based on the severity of the vulnerabilities Halborn was testing the program for.

4.1 DENIAL OF SERVICE

Description:

The DeBrige program's execute_external_call instruction allows for blocks of instructions to be executed together, this is done through setting the external instructions' execution policy to MandatoryBlock. Tests were done to see if it was possible to create a block of external instructions that could cause a denial of service.

Results:



```
running 1 test
-------------- TEST START --------------
2022-12-16 14:18:28,457 DEBUG [debridge_client::test_validator] Creating new test validator
2022-12-16 14:18:28,457 DEBUG [debridge_client::test_validator] Use target dir: "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/target"
2022-12-16 14:18:28,457 DEBUG [debridge_client::test_validator] Use ledger dir: "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/target/test-validator"
2022-12-16 14:18:28,458 DEBUG [debridge_client::test_validator] Start "solana-test-validator" "--ledger" "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/target/test-validator" "--mint" "DuFfamGLQEvPeToog1aFUfBohiRVTrGysaPiEkmEVE5s" "--bpf-program" "Fy8RGG
dge_settings_program.so" "--bpf-program" "9LiuUqoqBrXmM9iamBn7egcm83mx5dTRe1fCGRrSBeWT" "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/target/deploy/debridge_program.so" "--bpf-program" "SwaPpA9LAaLfeLi3a68M4DjnLqgtticKg6CnyNwgAC8" "/Users/michaelsmith/D
knL" "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/bin/spl_associated_token_account.so" "--bpf-program" "metaqbxxUerdq28cj1RbAWkYQm3ybzjb6a8bt518x1s" "/Users/michaelsmith/Documents/halborn_projects/solana-contracts/bin/mpl_token_metadata.so"
2022-12-16 14:18:28,461 DEBUG [debridge_client::test_validator] Connect to http://127.0.0.1:8899
2022-12-16 14:18:29,844 INFO [debridge_client::test_validator] Validator online
2022-12-16 14:18:29,845 INFO [functional_tests] Start airdrops
2022-12-16 14:18:29,870 INFO [functional_tests] Airdrop finished
2022-12-16 14:18:29,880 INFO [functional_tests] Start initialization of test oracles
2022-12-16 14:18:29,896 INFO [functional_tests] Deploy id of mint bridge fixture: dcef17fdca0a1020a69da8120ef5960cbdbd6d753c4b40068202d672e195364d
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: 561882be2686c7f3a8ab9156690a50d248474ee9 with signature: 0aa575ab48f81af022d1422b82585a79b8540ed7ec63170ec5254949ac89b9114df366542e763e143acebaee1c13dd2cf739ef66de2450
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: 377a5758ea017c170fb71abc4ee76005a4de8471 with signature: 4619f29a1a26772485c0847399fbd06461737089ab15448a410569d785e867ee052adb730b9e5313eda78ae42cf81eb973d4e19150fcad
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: d2ff827bddc6e94a90ff01a0e08a1d1b3f22e402 with signature: 087ba83a9318b3ebd91d80ea8c3221b7cf8294fee622e39ca2de8c14a3abec3e27ea52b6f7a1d7bd48cd65ea7aeda45d3dc31008191418
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: e633a09a9f01507a0ff3812e76637f04528e4f15 with signature: 671b8b631295d637daf60c06687faed2937f1331938db56fe0288881885dd6c02f0adcb09802c7f94ac25900b4b38a28f4f27a11292fc7
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: d96db3e2649ccba3ca88af2cdf6db2de5ebff873 with signature: 609fa5c67a26acd9118da862ef7f39406c5eb4dd6fdd660af4d7a9869f23df93082a6233c0aa0b4caf060ef2f9a9d25fbee1a9414eb23a
2022-12-16 14:18:29,911 DEBUG [debridge_client::client::settings_client] Store confirmation from oracle: 25fbb129053af6e081befdaf1f3e144e6ce771df with signature: f9be2767255018f09ddc25e66f7a2c0b10f9d3938fcbccbde75ec98c18aeb1a87709ce10a9398e75b7d5c20c7d4bd314a63d78c5e89ab6
2022-12-16 14:18:29,911 DEBUG [debridge_client::settings_instructions_builder] Secp256k1Instruction: Start construct instruction for 6 signatures
2022-12-16 14:18:29,911 DEBUG [debridge_client::settings_instructions_builder] Secp256k1Instruction: Full length of instruction_data will 638 bytes
2022-12-16 14:18:29,911 DEBUG [debridge_client::settings_instructions_builder] Secp256k1Instruction: offsets: [SecpSignatureOffsets { signature_offset: 147, signature_instruction_index: 0, eth_address_offset: 127, eth_address_instruction_index: 0, message_data_offset: 67,
index: 0, eth_address_offset: 212, eth_address_instruction_index: 0, message_data_offset: 67, message_data_size: 60, message_instruction_index: 0 }, SecpSignatureOffsets { signature_offset: 317, signature_instruction_index: 0, eth_address_offset: 297, eth_address_instruct
re_offset: 402, signature_instruction_index: 0, eth_address_offset: 382, eth_address_instruction_index: 0, message_data_offset: 67, message_data_size: 60, message_instruction_index: 0 }, SecpSignatureOffsets { signature_offset: 487, signature_instruction_index: 0, eth_add
x: 0 }, SecpSignatureOffsets { signature_offset: 572, signature_instruction_index: 0, eth_address_offset: 552, eth_address_instruction_index: 0, message_data_offset: 67, message_data_size: 60, message_instruction_index: 0 }] (67) with bytes [0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 25, 69, 116, 104, 101, 114, 101, 117, 109, 32, 83, 105, 103, 110, 101, 100, 32, 77, 101, 115, 115, 97, 103, 101, 58, 10, 51, 50, 220, 239, 23, 253, 202, 10, 16, 32, 166, 157, 168, 18, 14, 245, 150, 12, 189, 189, 109, 117, 60,
, 71, 78, 233, 10, 165, 117, 171, 72, 248, 26, 240, 34, 209, 66, 43, 130, 88, 90, 121, 184, 84, 14, 215, 236, 99, 23, 14, 197, 37, 73, 73, 172, 137, 185, 17, 77, 243, 102, 84, 46, 118, 62, 20, 58, 206, 186, 238, 28, 19, 221, 44, 247, 57, 239, 102, 222, 36, 80, 175, 202, 5
25, 242, 154, 26, 38, 119, 36, 133, 192, 132, 115, 153, 251, 208, 100, 97, 115, 112, 137, 171, 21, 68, 138, 65, 5, 105, 215, 133, 232, 103, 238, 5, 42, 219, 115, 11, 158, 83, 19, 237, 167, 138, 228, 44, 248, 30, 185, 115, 212, 225, 145, 80, 252, 173, 72, 116, 7, 63, 25, 1
58, 147, 24, 179, 235, 217, 29, 128, 234, 140, 50, 33, 183, 207, 130, 148, 254, 230, 34, 227, 156, 162, 222, 140, 20, 163, 171, 236, 62, 39, 234, 82, 182, 247, 161, 215, 189, 72, 205, 101, 234, 122, 237, 164, 93, 61, 195, 16, 8, 25, 20, 24, 115, 225, 180, 93, 181, 49, 32,
149, 214, 55, 218, 246, 12, 6, 104, 127, 174, 210, 147, 127, 19, 49, 147, 141, 181, 111, 224, 40, 136, 129, 136, 93, 214, 192, 47, 10, 220, 176, 152, 2, 199, 249, 74, 194, 89, 0, 180, 179, 138, 40, 244, 242, 122, 17, 41, 47, 199, 39, 45, 1, 150, 71, 252, 94, 69, 123, 0, 2
 172, 217, 17, 141, 168, 98, 239, 127, 57, 64, 108, 94, 180, 221, 111, 221, 102, 10, 244, 215, 169, 134, 159, 35, 223, 147, 8, 42, 98, 51, 192, 170, 11, 76, 175, 6, 14, 242, 249, 169, 210, 95, 190, 225, 169, 65, 78, 178, 58, 244, 212, 35, 105, 227, 210, 139, 25, 48, 1, 37
 157, 220, 37, 230, 111, 122, 44, 11, 16, 249, 211, 147, 143, 203, 204, 189, 231, 94, 201, 140, 24, 174, 177, 168, 119, 9, 206, 16, 169, 57, 142, 117, 183, 213, 194, 12, 125, 75, 211, 20, 166, 61, 120, 197, 232, 154, 182, 232, 226, 211, 77, 121, 150, 228, 120, 51, 1, 0]
2022-12-16 14:18:29,915 DEBUG [debridge_client::settings_instructions_builder] Secp256k1Instruction: ready instruction data [6, 147, 0, 0, 127, 0, 0, 67, 0, 60, 0, 0, 232, 0, 0, 212, 0, 0, 67, 0, 60, 0, 0, 61, 1, 0, 41, 1, 0, 67, 0, 60, 0, 0, 146, 1, 0, 126, 1, 0, 67, 0,
109, 32, 83, 105, 103, 110, 101, 100, 32, 77, 101, 115, 115, 97, 103, 101, 58, 10, 51, 50, 220, 239, 23, 253, 202, 10, 16, 32, 166, 157, 168, 18, 14, 245, 150, 12, 189, 189, 109, 117, 60, 75, 64, 6, 130, 2, 214, 114, 225, 149, 54, 77, 86, 24, 130, 190, 38, 134, 199, 243,
, 184, 84, 14, 215, 236, 99, 23, 14, 197, 37, 73, 73, 172, 137, 185, 17, 77, 243, 102, 84, 46, 118, 62, 20, 58, 206, 186, 238, 28, 19, 221, 44, 247, 57, 239, 102, 222, 36, 80, 175, 202, 50, 254, 90, 43, 108, 52, 51, 1, 55, 122, 87, 88, 234, 1, 124, 23, 15, 183, 26, 188, 7
137, 171, 21, 68, 138, 65, 5, 105, 215, 133, 232, 103, 238, 5, 42, 219, 115, 11, 158, 83, 19, 237, 167, 138, 228, 44, 248, 30, 185, 115, 212, 225, 145, 80, 252, 173, 72, 116, 7, 63, 25, 19, 220, 231, 15, 1, 210, 255, 130, 123, 221, 198, 233, 74, 144, 255, 1, 160, 224, 138
34, 227, 156, 162, 222, 140, 20, 163, 171, 236, 62, 39, 234, 82, 182, 247, 161, 215, 189, 72, 205, 101, 234, 122, 237, 164, 93, 61, 195, 16, 8, 25, 20, 24, 115, 225, 180, 93, 181, 49, 32, 206, 220, 0, 230, 51, 160, 154, 159, 1, 80, 122, 15, 243, 129, 46, 118, 99, 127, 4,
11, 224, 40, 136, 129, 136, 93, 214, 192, 47, 10, 220, 176, 152, 2, 199, 249, 74, 194, 89, 0, 180, 179, 138, 40, 244, 242, 122, 17, 41, 47, 199, 39, 45, 1, 150, 71, 252, 94, 69, 123, 0, 217, 109, 179, 226, 100, 156, 203, 163, 202, 136, 175, 44, 223, 109, 178, 222, 94, 191
244, 215, 169, 134, 159, 35, 223, 147, 8, 42, 98, 51, 192, 170, 11, 76, 175, 6, 14, 242, 249, 169, 210, 95, 190, 225, 169, 65, 78, 178, 58, 244, 212, 35, 105, 227, 210, 139, 25, 48, 1, 37, 251, 177, 41, 5, 58, 246, 224, 129, 190, 253, 175, 31, 62, 20, 78, 108, 231, 113, 2
 201, 140, 24, 174, 177, 168, 119, 9, 206, 16, 169, 57, 142, 117, 183, 213, 194, 12, 125, 75, 211, 20, 166, 61, 120, 197, 232, 154, 182, 232, 226, 211, 77, 121, 150, 228, 120, 51, 1, 0]
2022-12-16 14:18:29,920 DEBUG [debridge_client::client] Create transaction for [User] with ix: [Instruction { program_id: KeccakSecp256k11111111111111111111111111, accounts: [], data: [6, 147, 0, 0, 127, 0, 0, 67, 0, 60, 0, 0, 232, 0, 0, 212, 0, 0, 67, 0, 60, 0, 0, 61,
```

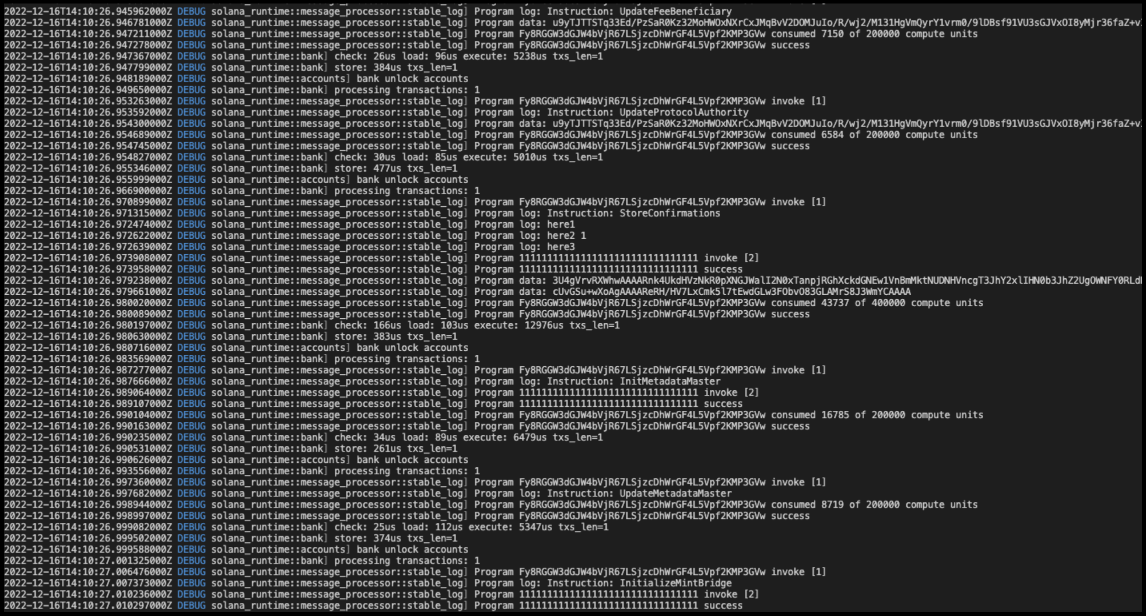
No code vulnerabilities were identified.

4.2 ACCESS CONTROL AND REGRESSION TESTING

Description:

In both the Debridge and settings program, new instructions were introduced and some updated to resolve access control vulnerabilities. These were tested to confirm no new vulnerabilities were introduced and that the previous fixes resolved the issue.

Results:



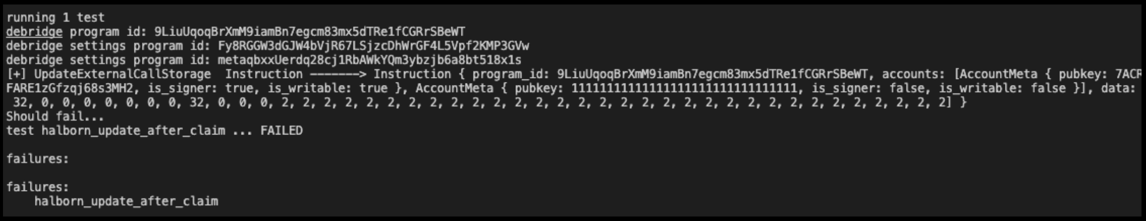
```
2022-12-16T14:10:26.945962000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: UpdateFeeBeneficiary
2022-12-16T14:10:26.946781000Z DEBUG solana_runtime::message_processor::stable_log] Program data: u9yTJTTSTq33Ed/PzSaR0Kz32MoHWOxNXrCxJMqBvV2DOMJuIo/R/wj2/M131HgVmQyrY1vrm0/9lDBsf91VU3sGJVxOI8yMjr36faZ+v
2022-12-16T14:10:26.947211000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw consumed 7150 of 200000 compute units
2022-12-16T14:10:26.947278000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw success
2022-12-16T14:10:26.947367000Z DEBUG solana_runtime::bank] check: 26us load: 96us execute: 5238us txs_len=1
2022-12-16T14:10:26.947799000Z DEBUG solana_runtime::bank] store: 384us txs_len=1
2022-12-16T14:10:26.948189000Z DEBUG solana_runtime::accounts] bank unlock accounts
2022-12-16T14:10:26.949650000Z DEBUG solana_runtime::bank] processing transactions: 1
2022-12-16T14:10:26.953263000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw invoke [1]
2022-12-16T14:10:26.953592000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: UpdateProtocolAuthority
2022-12-16T14:10:26.954300000Z DEBUG solana_runtime::message_processor::stable_log] Program data: u9yTJTTSTq33Ed/PzSaR0Kz32MoHWOxNXrCxJMqBvV2DOMJuIo/R/wj2/M131HgVmQyrY1vrm0/9lDBsf91VU3sGJVxOI8yMjr36faZ+v
2022-12-16T14:10:26.954689000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw consumed 6584 of 200000 compute units
2022-12-16T14:10:26.954745000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw success
2022-12-16T14:10:26.954827000Z DEBUG solana_runtime::bank] check: 30us load: 85us execute: 5010us txs_len=1
2022-12-16T14:10:26.955346000Z DEBUG solana_runtime::bank] store: 477us txs_len=1
2022-12-16T14:10:26.955999000Z DEBUG solana_runtime::accounts] bank unlock accounts
2022-12-16T14:10:26.966900000Z DEBUG solana_runtime::bank] processing transactions: 1
2022-12-16T14:10:26.970899000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw invoke [1]
2022-12-16T14:10:26.971315000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: StoreConfirmations
2022-12-16T14:10:26.972474000Z DEBUG solana_runtime::message_processor::stable_log] Program log: here1
2022-12-16T14:10:26.972622000Z DEBUG solana_runtime::message_processor::stable_log] Program log: here2 1
2022-12-16T14:10:26.972639000Z DEBUG solana_runtime::message_processor::stable_log] Program log: here3
2022-12-16T14:10:26.973908000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 invoke [2]
2022-12-16T14:10:26.973958000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 success
2022-12-16T14:10:26.979238000Z DEBUG solana_runtime::message_processor::stable_log] Program data: 3U4gVrvRXWhwAAAARnk4UkdHVzNkR0pXNGJWalI2N0xTanpjRGhXckdGNEw1VnBmMktNUDNHVncgT3JhY2xlIHN0b3JhZ2UgOWNFY0RLdl
2022-12-16T14:10:26.979661000Z DEBUG solana_runtime::message_processor::stable_log] Program data: cUvGSu+wXoAgAAAAReRH/HV7LxCmk5l7tEwdGLw3FObvO83GLAMrS8J3WmYCAAAA
2022-12-16T14:10:26.980020000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw consumed 43737 of 400000 compute units
2022-12-16T14:10:26.980089000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw success
2022-12-16T14:10:26.980197000Z DEBUG solana_runtime::bank] check: 166us load: 103us execute: 12976us txs_len=1
2022-12-16T14:10:26.980630000Z DEBUG solana_runtime::bank] store: 383us txs_len=1
2022-12-16T14:10:26.980716000Z DEBUG solana_runtime::accounts] bank unlock accounts
2022-12-16T14:10:26.983569000Z DEBUG solana_runtime::bank] processing transactions: 1
2022-12-16T14:10:26.987277000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw invoke [1]
2022-12-16T14:10:26.987666000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: InitMetadataMaster
2022-12-16T14:10:26.989064000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 invoke [2]
2022-12-16T14:10:26.989107000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 success
2022-12-16T14:10:26.990104000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw consumed 16785 of 200000 compute units
2022-12-16T14:10:26.990163000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw success
2022-12-16T14:10:26.990235000Z DEBUG solana_runtime::bank] check: 34us load: 89us execute: 6479us txs_len=1
2022-12-16T14:10:26.990531000Z DEBUG solana_runtime::bank] store: 261us txs_len=1
2022-12-16T14:10:26.990626000Z DEBUG solana_runtime::accounts] bank unlock accounts
2022-12-16T14:10:26.993556000Z DEBUG solana_runtime::bank] processing transactions: 1
2022-12-16T14:10:26.997360000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw invoke [1]
2022-12-16T14:10:26.997682000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: UpdateMetadataMaster
2022-12-16T14:10:26.998944000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw consumed 8719 of 200000 compute units
2022-12-16T14:10:26.998997000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw success
2022-12-16T14:10:26.999082000Z DEBUG solana_runtime::bank] check: 25us load: 112us execute: 5347us txs_len=1
2022-12-16T14:10:26.999502000Z DEBUG solana_runtime::bank] store: 374us txs_len=1
2022-12-16T14:10:26.999588000Z DEBUG solana_runtime::accounts] bank unlock accounts
2022-12-16T14:10:27.001325000Z DEBUG solana_runtime::bank] processing transactions: 1
2022-12-16T14:10:27.006476000Z DEBUG solana_runtime::message_processor::stable_log] Program Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw invoke [1]
2022-12-16T14:10:27.007373000Z DEBUG solana_runtime::message_processor::stable_log] Program log: Instruction: InitializeMintBridge
2022-12-16T14:10:27.010236000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 invoke [2]
2022-12-16T14:10:27.010297000Z DEBUG solana_runtime::message_processor::stable_log] Program 11111111111111111111111111111111 success
```

No code vulnerabilities were identified.

4.3 UPDATING EXTERNAL CALL STORAGE AFTER CLAIM

After a user submits a claim if there are any instructions in the external_call_storage it should be locked and available for executors to execute the instructions. Testing was done to confirm that the lock works as intended and the user is unable to execute the update_external_call function.

Results:


```
running 1 test
debridge program id: 9LiuUqoqBrXmM9iamBn7egcm83mx5dTRe1fCGRrSBeWT
debridge settings program id: Fy8RGGW3dGJW4bVjR67LSjzcDhWrGF4L5Vpf2KMP3GVw
debridge settings program id: metaqbxxUerdq28cj1RbAWkYQm3ybzjb6a8bt518x1s
[+] UpdateExternalCallStorage  Instruction -------> Instruction { program_id: 9LiuUqoqBrXmM9iamBn7egcm83mx5dTRe1fCGRrSBeWT, accounts: [AccountMeta { pubkey: 7ACR
FARE1zGfzqj68s3MH2, is_signer: true, is_writable: true }, AccountMeta { pubkey: 11111111111111111111111111111111, is_signer: false, is_writable: false }], data:
 32, 0, 0, 0, 0, 0, 0, 0, 32, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2] }
Should fail...
test halborn_update_after_claim ... FAILED

failures:

failures:
    halborn_update_after_claim
```

No code vulnerabilities were identified.

AUTOMATED TESTING

5.1 AUTOMATED ANALYSIS

Description:

Halborn used automated security scanners to assist with the detection of well-known security issues and vulnerabilities. Among the tools used was cargo-audit, a security scanner for vulnerabilities reported to the Rust-Sec Advisory Database. All vulnerabilities published in https://crates.io are stored in a repository named The RustSec Advisory Database. cargo audit is a human-readable version of the advisory database which performs a scanning on Cargo.lock. Security Detections are only in scope. All vulnerabilities shown here were already disclosed in the above report. However, to better assist the developers maintaining this code, the auditors are including the output with the dependencies tree, and this is included in the cargo audit output to better know the dependencies affected by unmaintained and vulnerable crates.

Results:

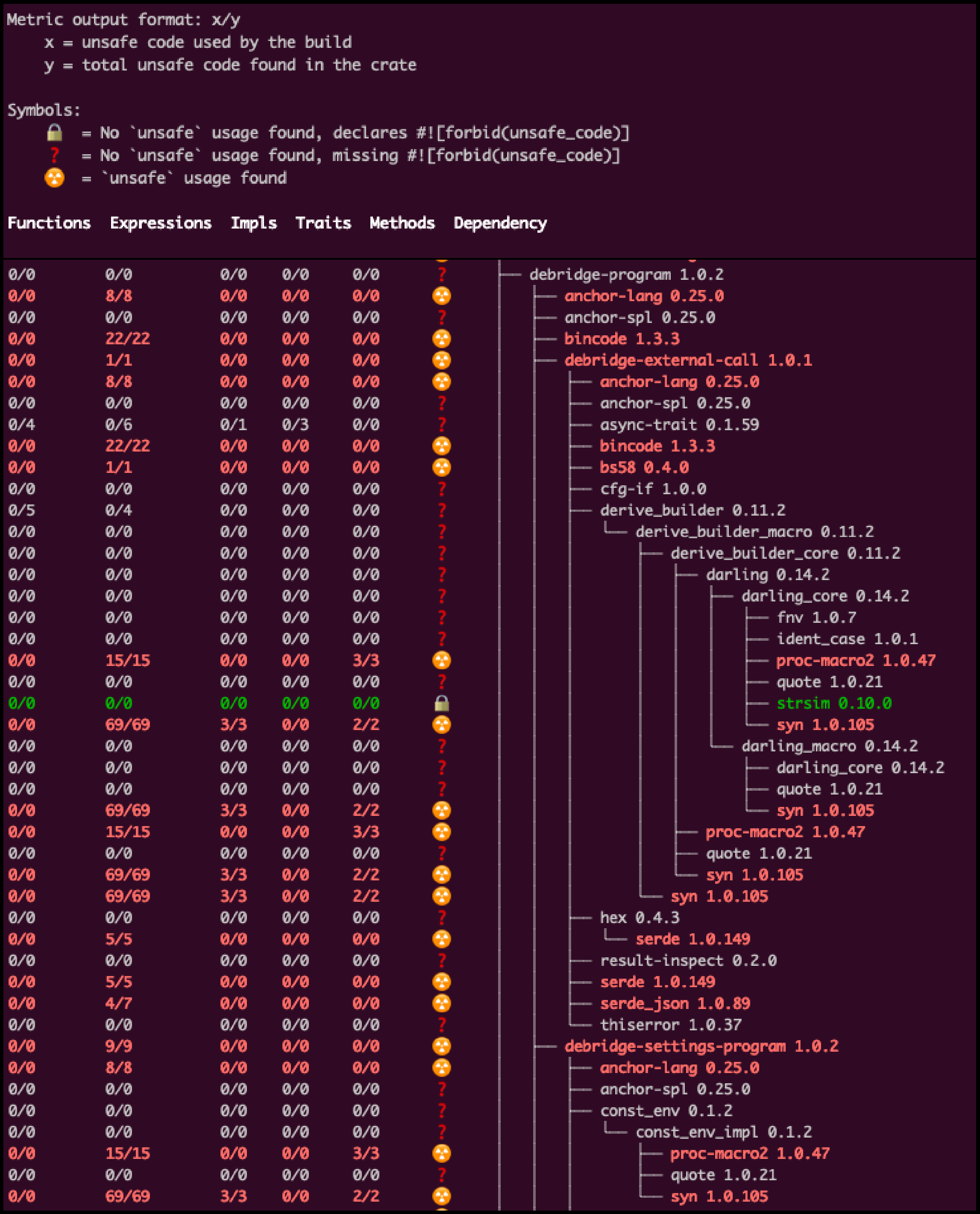
ID	package	short description
RUSTSEC-2020-0036	time	Potential segfault
RUSTSEC-2021-0139	ansi_term	Unmaintained

5.2 UNSAFE RUST CODE DETECTION

Description:

Halborn used automated security scanners to assist with the detection of well-known security issues and vulnerabilities. Among the tools used was cargo-geiger, a security tool that lists statistics related to the usage of unsafe Rust code in a core Rust codebase and all its dependencies.

Results:



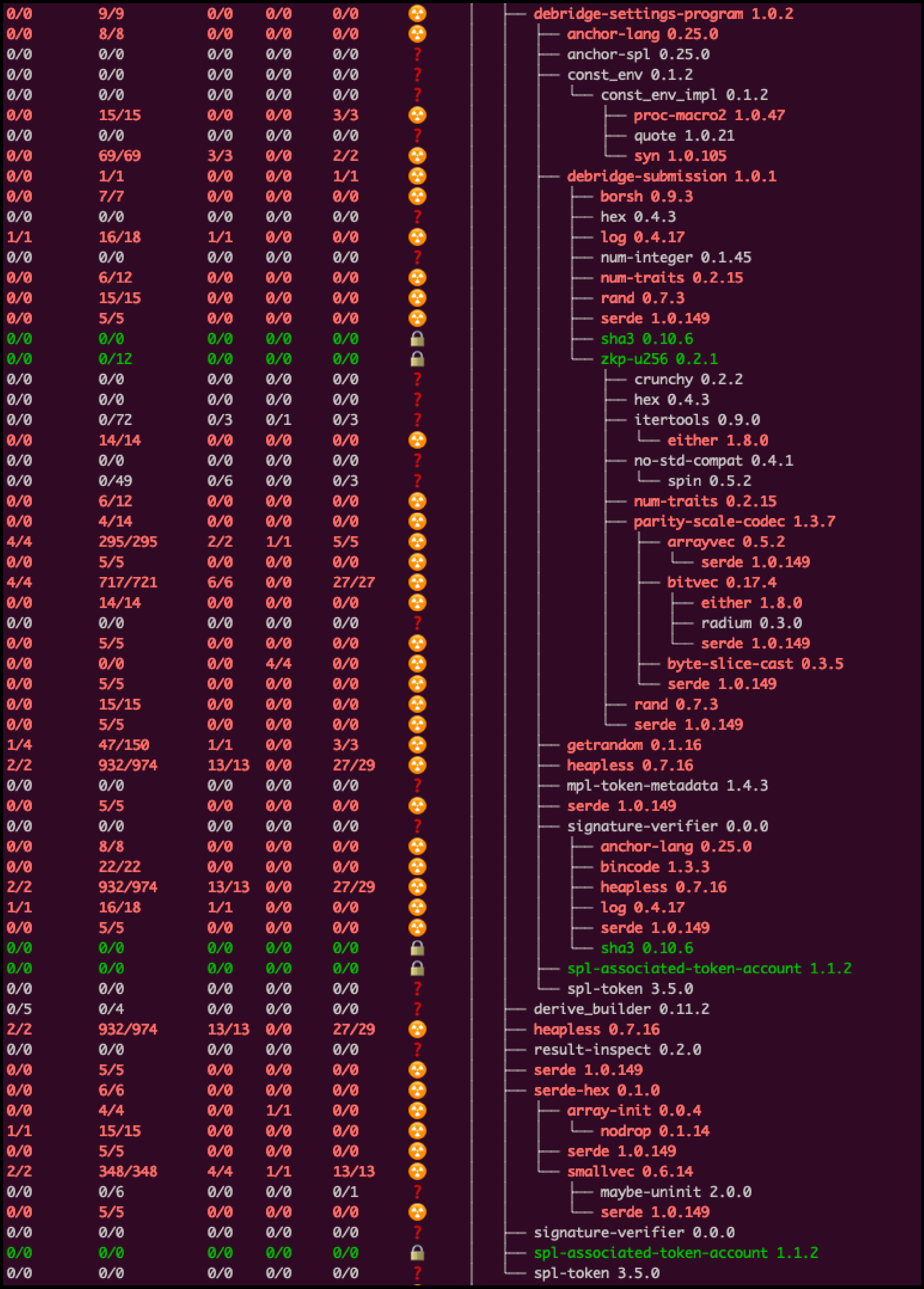
```
Metric output format: x/y
    x = unsafe code used by the build
    y = total unsafe code found in the crate

Symbols:
    🔒  = No `unsafe` usage found, declares #![forbid(unsafe_code)]
    ❓  = No `unsafe` usage found, missing #![forbid(unsafe_code)]
    ☢️  = `unsafe` usage found

Functions  Expressions  Impls  Traits  Methods  Dependency

0/0        0/0          0/0    0/0     0/0      ❓  ├── debridge-program 1.0.2
0/0        8/8          0/0    0/0     0/0      ☢️  │   ├── anchor-lang 0.25.0
0/0        0/0          0/0    0/0     0/0      ❓  │   ├── anchor-spl 0.25.0
0/0        22/22        0/0    0/0     0/0      ☢️  │   ├── bincode 1.3.3
0/0        1/1          0/0    0/0     0/0      ☢️  │   ├── debridge-external-call 1.0.1
0/0        8/8          0/0    0/0     0/0      ☢️  │   │   ├── anchor-lang 0.25.0
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── anchor-spl 0.25.0
0/4        0/6          0/1    0/3     0/0      ❓  │   │   ├── async-trait 0.1.59
0/0        22/22        0/0    0/0     0/0      ☢️  │   │   ├── bincode 1.3.3
0/0        1/1          0/0    0/0     0/0      ☢️  │   │   ├── bs58 0.4.0
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── cfg-if 1.0.0
0/5        0/4          0/0    0/0     0/0      ❓  │   │   ├── derive_builder 0.11.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   └── derive_builder_macro 0.11.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       ├── derive_builder_core 0.11.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   ├── darling 0.14.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │   ├── darling_core 0.14.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │   │   ├── fnv 1.0.7
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │   │   ├── ident_case 1.0.1
0/0        15/15        0/0    0/0     3/3      ☢️  │   │   │       │   │   │   ├── proc-macro2 1.0.47
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │   │   ├── quote 1.0.21
0/0        0/0          0/0    0/0     0/0      🔒  │   │   │       │   │   │   ├── strsim 0.10.0
0/0        69/69        3/3    0/0     2/2      ☢️  │   │   │       │   │   │   └── syn 1.0.105
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │   └── darling_macro 0.14.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │       ├── darling_core 0.14.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   │       ├── quote 1.0.21
0/0        69/69        3/3    0/0     2/2      ☢️  │   │   │       │   │       └── syn 1.0.105
0/0        15/15        0/0    0/0     3/3      ☢️  │   │   │       │   ├── proc-macro2 1.0.47
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       │   ├── quote 1.0.21
0/0        69/69        3/3    0/0     2/2      ☢️  │   │   │       │   └── syn 1.0.105
0/0        69/69        3/3    0/0     2/2      ☢️  │   │   │       └── syn 1.0.105
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── hex 0.4.3
0/0        5/5          0/0    0/0     0/0      ☢️  │   │   │   └── serde 1.0.149
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── result-inspect 0.2.0
0/0        5/5          0/0    0/0     0/0      ☢️  │   │   ├── serde 1.0.149
0/0        4/7          0/0    0/0     0/0      ☢️  │   │   ├── serde_json 1.0.89
0/0        0/0          0/0    0/0     0/0      ❓  │   │   └── thiserror 1.0.37
0/0        9/9          0/0    0/0     0/0      ☢️  │   ├── debridge-settings-program 1.0.2
0/0        8/8          0/0    0/0     0/0      ☢️  │   │   ├── anchor-lang 0.25.0
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── anchor-spl 0.25.0
0/0        0/0          0/0    0/0     0/0      ❓  │   │   ├── const_env 0.1.2
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │   └── const_env_impl 0.1.2
0/0        15/15        0/0    0/0     3/3      ☢️  │   │   │       ├── proc-macro2 1.0.47
0/0        0/0          0/0    0/0     0/0      ❓  │   │   │       ├── quote 1.0.21
0/0        69/69        3/3    0/0     2/2      ☢️  │   │   │       └── syn 1.0.105
```

AUTOMATED TESTING



```
0/0   9/9       0/0    0/0   0/0    ☢  ├── debridge-settings-program 1.0.2
0/0   8/8       0/0    0/0   0/0    ☢  │   ├── anchor-lang 0.25.0
0/0   0/0       0/0    0/0   0/0    ?  │   ├── anchor-spl 0.25.0
0/0   0/0       0/0    0/0   0/0    ?  │   ├── const_env 0.1.2
0/0   0/0       0/0    0/0   0/0    ?  │   │   └── const_env_impl 0.1.2
0/0   15/15     0/0    0/0   3/3    ☢  │   │       ├── proc-macro2 1.0.47
0/0   0/0       0/0    0/0   0/0    ?  │   │       ├── quote 1.0.21
0/0   69/69     3/3    0/0   2/2    ☢  │   │       └── syn 1.0.105
0/0   1/1       0/0    0/0   1/1    ☢  │   ├── debridge-submission 1.0.1
0/0   7/7       0/0    0/0   0/0    ☢  │   │   ├── borsh 0.9.3
0/0   0/0       0/0    0/0   0/0    ?  │   │   ├── hex 0.4.3
1/1   16/18     1/1    0/0   0/0    ☢  │   │   ├── log 0.4.17
0/0   0/0       0/0    0/0   0/0    ?  │   │   ├── num-integer 0.1.45
0/0   6/12      0/0    0/0   0/0    ☢  │   │   ├── num-traits 0.2.15
0/0   15/15     0/0    0/0   0/0    ☢  │   │   ├── rand 0.7.3
0/0   5/5       0/0    0/0   0/0    ☢  │   │   ├── serde 1.0.149
0/0   0/0       0/0    0/0   0/0    🔒 │   │   ├── sha3 0.10.6
0/0   0/12      0/0    0/0   0/0    🔒 │   │   └── zkp-u256 0.2.1
0/0   0/0       0/0    0/0   0/0    ?  │   │       ├── crunchy 0.2.2
0/0   0/0       0/0    0/0   0/0    ?  │   │       ├── hex 0.4.3
0/0   0/72      0/3    0/1   0/3    ?  │   │       ├── itertools 0.9.0
0/0   14/14     0/0    0/0   0/0    ☢  │   │       │   └── either 1.8.0
0/0   0/0       0/0    0/0   0/0    ?  │   │       ├── no-std-compat 0.4.1
0/0   0/49      0/6    0/0   0/3    ?  │   │       │   └── spin 0.5.2
0/0   6/12      0/0    0/0   0/0    ☢  │   │       ├── num-traits 0.2.15
0/0   4/14      0/0    0/0   0/0    ☢  │   │       ├── parity-scale-codec 1.3.7
4/4   295/295   2/2    1/1   5/5    ☢  │   │       │   ├── arrayvec 0.5.2
0/0   5/5       0/0    0/0   0/0    ☢  │   │       │   │   └── serde 1.0.149
4/4   717/721   6/6    0/0   27/27  ☢  │   │       │   ├── bitvec 0.17.4
0/0   14/14     0/0    0/0   0/0    ☢  │   │       │   │   ├── either 1.8.0
0/0   0/0       0/0    0/0   0/0    ?  │   │       │   │   ├── radium 0.3.0
0/0   5/5       0/0    0/0   0/0    ☢  │   │       │   │   └── serde 1.0.149
0/0   0/0       0/0    4/4   0/0    ☢  │   │       │   ├── byte-slice-cast 0.3.5
0/0   5/5       0/0    0/0   0/0    ☢  │   │       │   └── serde 1.0.149
0/0   15/15     0/0    0/0   0/0    ☢  │   │       ├── rand 0.7.3
0/0   5/5       0/0    0/0   0/0    ☢  │   │       └── serde 1.0.149
1/4   47/150    1/1    0/0   3/3    ☢  │   ├── getrandom 0.1.16
2/2   932/974   13/13  0/0   27/29  ☢  │   ├── heapless 0.7.16
0/0   0/0       0/0    0/0   0/0    ?  │   ├── mpl-token-metadata 1.4.3
0/0   5/5       0/0    0/0   0/0    ☢  │   ├── serde 1.0.149
0/0   0/0       0/0    0/0   0/0    ?  │   ├── signature-verifier 0.0.0
0/0   8/8       0/0    0/0   0/0    ☢  │   │   ├── anchor-lang 0.25.0
0/0   22/22     0/0    0/0   0/0    ☢  │   │   ├── bincode 1.3.3
2/2   932/974   13/13  0/0   27/29  ☢  │   │   ├── heapless 0.7.16
1/1   16/18     1/1    0/0   0/0    ☢  │   │   ├── log 0.4.17
0/0   5/5       0/0    0/0   0/0    ☢  │   │   ├── serde 1.0.149
0/0   0/0       0/0    0/0   0/0    🔒 │   │   └── sha3 0.10.6
0/0   0/0       0/0    0/0   0/0    🔒 │   ├── spl-associated-token-account 1.1.2
0/0   0/0       0/0    0/0   0/0    ?  │   └── spl-token 3.5.0
0/5   0/4       0/0    0/0   0/0    ?  ├── derive_builder 0.11.2
2/2   932/974   13/13  0/0   27/29  ☢  ├── heapless 0.7.16
0/0   0/0       0/0    0/0   0/0    ?  ├── result-inspect 0.2.0
0/0   5/5       0/0    0/0   0/0    ☢  ├── serde 1.0.149
0/0   6/6       0/0    0/0   0/0    ☢  ├── serde-hex 0.1.0
0/0   4/4       0/0    1/1   0/0    ☢  │   ├── array-init 0.0.4
1/1   15/15     0/0    0/0   0/0    ☢  │   │   └── nodrop 0.1.14
0/0   5/5       0/0    0/0   0/0    ☢  │   ├── serde 1.0.149
2/2   348/348   4/4    1/1   13/13  ☢  │   └── smallvec 0.6.14
0/0   0/6       0/0    0/0   0/1    ?  │       ├── maybe-uninit 2.0.0
0/0   5/5       0/0    0/0   0/0    ☢  │       └── serde 1.0.149
0/0   0/0       0/0    0/0   0/0    ?  ├── signature-verifier 0.0.0
0/0   0/0       0/0    0/0   0/0    🔒 ├── spl-associated-token-account 1.1.2
0/0   0/0       0/0    0/0   0/0    ?  └── spl-token 3.5.0
```

THANK YOU FOR CHOOSING

HALBORN