Orderly Protocol - Contracts

NEAR Smart Contract Security Audit

Prepared by: **Halborn**

Date of Engagement: **May 30th, 2022 - June 16th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	05/30/2022	Jose C. Ramirez
0.2	Document Edits	06/16/2022	Lukasz Mikula
0.3	Draft Edits	06/20/2022	Timur Guvenkaya
0.4	Draft Review	06/20/2022	Gabi Urrutia
1.0	Remediation Plan	09/20/2022	Lukasz Mikula
1.1	Remediation Plan Review	09/20/2022	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
Timur Guvenkaya	Halborn	Timur.Guvenkaya@halborn.com

Jose C. Ramirez	Halborn	Jose.Ramirez@halborn.com
Lukasz Mikula	Halborn	Lukasz.Mikula@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

Orderly Protocol engaged Halborn to conduct a security audit on their smart contracts beginning on May 30th, 2022 and ending on June 16th, 2022 . The security assessment was scoped to the smart contracts provided in the GitHub repository Orderly Protocol, 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 two weeks for the engagement and assigned two full-time security engineers to audit the security of the smart contract. The security engineers are blockchain and smart-contract security experts with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The purpose of this audit is to:

- Ensure that smart contract functions operate as intended
- Identify potential security issues with the smart contracts

In summary, Halborn identified some improvements to reduce the likelihood and impact of risks, which were mostly addressed by Orderly Protocol . The main ones are the following:

- Enforced fee_collector checks on each function that leads to account creation process
- Users withdrawal are released after certain period of time if the operator is idle
- Improved ownership transfer process has been introduced
- A check has been implemented to prevent accounts to have multiple privileged roles at once
- Improved validation of trade pairs has been introduced to avoid e. g. overwriting old pairs or adding malicious pairs.

1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual review of the code and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of the smart contract audit. While manual testing is recommended to uncover flaws in logic, process, and implementation; automated testing techniques help enhance coverage of smart contracts 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:

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

- Research into the architecture, purpose, and use of the platform.
- Smart contract manual code review and walk-through to identify any logic issue.
- Thorough assessment of safety and usage of critical Rust variables and functions in scope that could led to arithmetic related vulnerabilities.
- Finding unsafe Rust code usage (cargo-geiger)
- Test coverage review (cargo tarpaulin).
- On chain testing of core functions(near-cli, NEAR-API-JS)
- Deployment of Smart Contracts (kurtosis, near localnet)
- Scanning of Rust dependencies for known vulnerabilities (cargo audit).

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 repository: https://gitlab.com/orderly-network/protocol

1. NEAR Orderly Protocol Smart Contract

    (a) Commit ID: df1e384d9854905415bd203087820a624abde4071

    (b) Contracts in scope:

    - contract_utils.rs
    - contract.rs
    - event.rs
    - lib.rs
    - operator.rs
    - owner.rs
    - tests.rs
    - token_balance.rs
    - types.rs

Out-of-scope: External libraries and financial related attacks.

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	2	4	1	2

LIKELIHOOD

IMPACT

🟨	🟨 (HAL-05) (HAL-06)	🟥	🟥	🟪
🟩 (HAL-07)	🟨 (HAL-04)	🟨 (HAL-03)	🟥 (HAL-01)	🟥
🟩	🟩	🟨	🟨	🟥 (HAL-02)
⬜	🟩	🟩	🟨	🟨
⬜ (HAL-08) (HAL-09)	⬜	🟩	🟩	🟨

EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
HAL01 - FEE COLLECTOR COULD BE REGISTERED AS USER	High	SOLVED - 20/09/2022
HAL02 - USERS CANNOT RETRIEVE THEIR FUNDS WITHOUT OPERATOR'S APPROVAL	High	SOLVED - 20/09/2022
HAL03 - WEAK PRIVILEGE SEPARATION	Medium	SOLVED - 20/09/2022
HAL04 - PRIVILEGED ADDRESS CAN BE TRANSFERRED WITHOUT CONFIRMATION	Medium	SOLVED - 20/09/2022
HAL05 - INSECURE PAIRS MANAGEMENT LOGIC	Medium	SOLVED - 20/09/2022
HAL06 - EXCESSIVELY CENTRALIZED FEATURES	Medium	SOLVED - 20/09/2022
HAL07 - MISSING AUTHORIZATION CHECK	Low	SOLVED - 20/09/2022
HAL08 - REDUNDANT CODE	Informational	SOLVED - 20/09/2022
HAL09 - OPERATOR KEY IS NOT DELETED ON OPERATOR CHANGE	Informational	ACKNOWLEDGED

FINDINGS & TECH DETAILS

3.1 (HAL-01) FEE COLLECTOR COULD BE REGISTERED AS USER - HIGH

Description:

The create_user_account successfully enforces multiple restrictions on newly created user, such as not being the fee_collector and the caller being the signer of the transaction. However, this restriction could be bypassed, as the user_deposit_token function will add any depositor to the users list just by checking that they are not already part of it.

In this way, the fee_collector could sign itself as a user just by depositing through the user_deposit_native_token function.

In order to create a user who is a fee_collector in the same time, one has to:

- create a legitimate fee_collector, and then
- perform a deposit to have an account created

Below snippet shows the code responsible for the issue:

Code Location:

Listing 1: src/contract.rs (Line 408)

```
#[payable]
pub fn user_deposit_native_token(&mut self) {
    let user = env::predecessor_account_id();
    let amount = env::attached_deposit();
    self.user_deposit_token(user, NATIVE_TOKEN.parse().unwrap(), amount);
}

fn user_deposit_token(&mut self, user: AccountId, token: AccountId, amount: u128) {
    if amount == 0 {
        // don't bother creating useless state and emitting
```

```
 ↳ unnecessary event
            return;
        }

        if !self.users.contains(&user) {
            self.users.insert(&user);
            Self::emit_event(Event::CreateUserAccount(user.clone()));
        }

```

Risk Level:

Likelihood - 4
Impact - 4

Recommendation:

Modify the user_deposit_token function, so it calls create_user_account for users that are not already registered instead of adding them directly to the list.

Remediation plan:

SOLVED: The issue was solved in commit 11a5ae159463086741141083ae86e30e80fad69a by adding another check if the user about to be added is not already a fee collector.

3.2 (HAL-02) USERS CANNOT RETRIEVE THEIR FUNDS WITHOUT OPERATOR'S APPROVAL - HIGH

Description:

The architecture of asset-manager allows for user withdrawals only if they are requested by users and approved by operator_manager. However, there is no possibility for users to retrieve their funds if the operator do not approve the withdrawal request.

This might lead to disallowing users to reclaim their funds against their will in some situations. The withdrawal process is as follows:

- user create withdraw request
- the request is either approved and funds are released,
- or the withdrawal is performed by operator and in such case it can't exceed requested amount

Code Location:

Listing 2: src/contract.rs (Lines 139,140)

```
pub fn user_request_withdraw(&mut self, token: AccountId, amount: U128) {
        let amount = amount.0;
        let user = env::predecessor_account_id();

        if amount == 0 {
            // don't bother creating useless state and emitting unnecessary event
            return;
        }

        if self
            .user_withdraw_requests
            .contains_key(&user_token_to_key(&user, &token))
        {
            env::panic_str("User had already created a withdraw request for this token");
        }

        let token_balance = self.user_token_balance(user.clone(), token.clone()).0;

        if token_balance < amount {
            env::panic_str("Insufficient token balance");
        }

        let request = WithdrawRequest {
            amount: amount.into(),
            request_time: env::block_timestamp(),
        };

        self.user_withdraw_requests
            .insert(&user_token_to_key(&user, &token), &request);

        Self::emit_event(Event::WithdrawRequest {
            user,
            token,
            amount: amount.into(),
        })
    }
```

Risk Level:

Likelihood - 5

Impact - 3

Recommendation:

It is recommended to introduce a method for users to retrieve their funds. In case e.g. lost to operator account is lost or a malicious actor using it, the funds might never be returned to users. One of the possibilities might be to release these funds without approval after certain period of lockout time, similarly to e.g. staking mechanisms.

Remediation plan:

SOLVED: The issue was solved in commit 11a5ae1594630867411410 83ae86e30e80fad69a by adding the ability to perform manual withdrawals after the maximum operator idle time is exceeded.

3.3 (HAL-03) WEAK PRIVILEGE SEPARATION - MEDIUM

Description:

It was observed that the owner could set itself as a operator_manager and fee_collector, both upon initialization and through “set” functions. This functionality violates the principle of least privilege giving the owner additional privileges. Moreover, the owner has a possibility of changing operator_manager and fee_collector which grants him absolute control over the whole contract.

Code Location:

Listing 3: src/owner.rs (Line 18)

```
18 pub fn set_owner(&mut self, owner: AccountId) {
19     self.assert_owner();
20     self.owner = owner;
21 }
```

Listing 4: src/owner.rs (Line 32)

```
32 pub fn set_operator_manager(&mut self, operator_manager: AccountId
 ↳ ) {
33     self.assert_owner_or_operator();
34     self.operator_manager = operator_manager;
35 }
```

Listing 5: src/contract.rs (Line 338)

```
338 pub fn set_fee_collector(&mut self, fee_collector: AccountId) {
339     self.assert_owner_or_operator();
340     if self.users.contains(&fee_collector) {
341         env::panic_str("fee collector can't be a trading account")
 ↳ ;
342     }
343     let old_collector = self.fee_collector.clone();
344     if fee_collector == old_collector {
345         return;
346     }
347
348     self.fee_collector = fee_collector;
349 }
```

Listing 6: src/contract.rs (Line 66)

```
66 #[init]
67 pub fn new(owner: AccountId, operator_manager: AccountId, fee_collector: AccountId) -> Self {//@audit-ok
68     Self {
69         owner,
70         operator_manager,
71         operator_access_key: None,
72         users: LookupSet::new(StorageKey::Users),
73         user_keys: UnorderedMap::new(StorageKey::UserKeys),
74         user_token_balances: UnorderedMap::new(StorageKey::UserTokenBalances),
75         user_withdraw_requests: LookupMap::new(StorageKey::UserWithdrawRequests),
76         pairs_tokens_whitelist: LookupMap::new(StorageKey::PairsTokensWhitelist),
77         tokens_whitelist: UnorderedSet::new(StorageKey::TokensWhitelist),
78         fee_collector,
79         fee_collector_balance: LookupMap::new(StorageKey::FeeCollectorBalance),
80     }
81 }
```

Risk Level:

Likelihood - 3
Impact - 4

Recommendation:

It is recommended to add another check to not allow the owner to set itself as operator_manager or fee_collector and separate the roles from itself, so each of them is managed by itself instead of all being managed by the owner.

Remediation plan:

SOLVED: The issue was solved in commit 11a5ae1594630867411410 83ae86e30e80fad69a by adding additional checks if certain account already has other privileges enabled.

3.4 (HAL-04) PRIVILEGED ADDRESS CAN BE TRANSFERRED WITHOUT CONFIRMATION - MEDIUM

Description:

An incorrect use of the set_owner or set_operator_manager functions from the contract could set the affected privileged roles to an incorrect address, unwillingly losing control of the contract, which cannot be undone in any way. Currently, the owner and operator_manager of the contract can change their addresses using the aforementioned function in a single transaction and without confirmation from the new address.

Code Location:

Listing 7: src/owner.rs (Line 18)

```rust
pub fn set_owner(&mut self, owner: AccountId) {
    self.assert_owner();
    self.owner = owner;
}
```

Listing 8: src/owner.rs (Line 32)

```rust
pub fn set_operator_manager(&mut self, operator_manager: AccountId
) {
    self.assert_owner_or_operator();
    self.operator_manager = operator_manager;
}
```

Risk Level:

Likelihood - 2
Impact - 4

Recommendation:

The set_owner or set_operator_manager functions should follow a two steps process, being split into set_owner and accept_owner functions. The latter one requiring the transfer to be completed by the recipient, effectively protecting the contract against potential typing errors compared to single-step role transfer mechanisms.

Remediation plan:

SOLVED: The issue was solved in commit 11a5ae159463086741141083ae86e30e80fad69a by adding additional approve_request logic.

3.5 (HAL-05) INSECURE PAIRS MANAGEMENT LOGIC - MEDIUM

Description:

The logic of adding new pairs to pairs_tokens_whitelist includes several features, which might lead to confusion and/or security vulnerabilities. These are as follows:

- there is no validation check if the pair that is being added already exists, if so, the old pair will be overwritten without notification (the name will become the same, but the tokens it holds will be overwritten)
- there is no token validation if tokens (account ids) in a pair differs, so it is possible to add pairs AA like BTCBTC or USDCUSDC. It was proven in different projects in the past that such behavior might lead to draining funds via price-based attacks if price calculation between asset is performed (e.g. on external AMM)
- the pairs cannot be removed once added
- there is no case normalization check which means that e.g. "BTCUSDT" and "BtCUSDT" will be considered different pairs. This might lead to confusion in future usage.
- Moreover, the pair name can contain non-alphanumeric characters, which might lead to web2 vulnerabilities like Cross-Site Scripting, Template Injections, or more sophisticated attacks.

Below is the responsible code snippet followed by a unit test has been developed in order to reproduce the issue and show results as output:

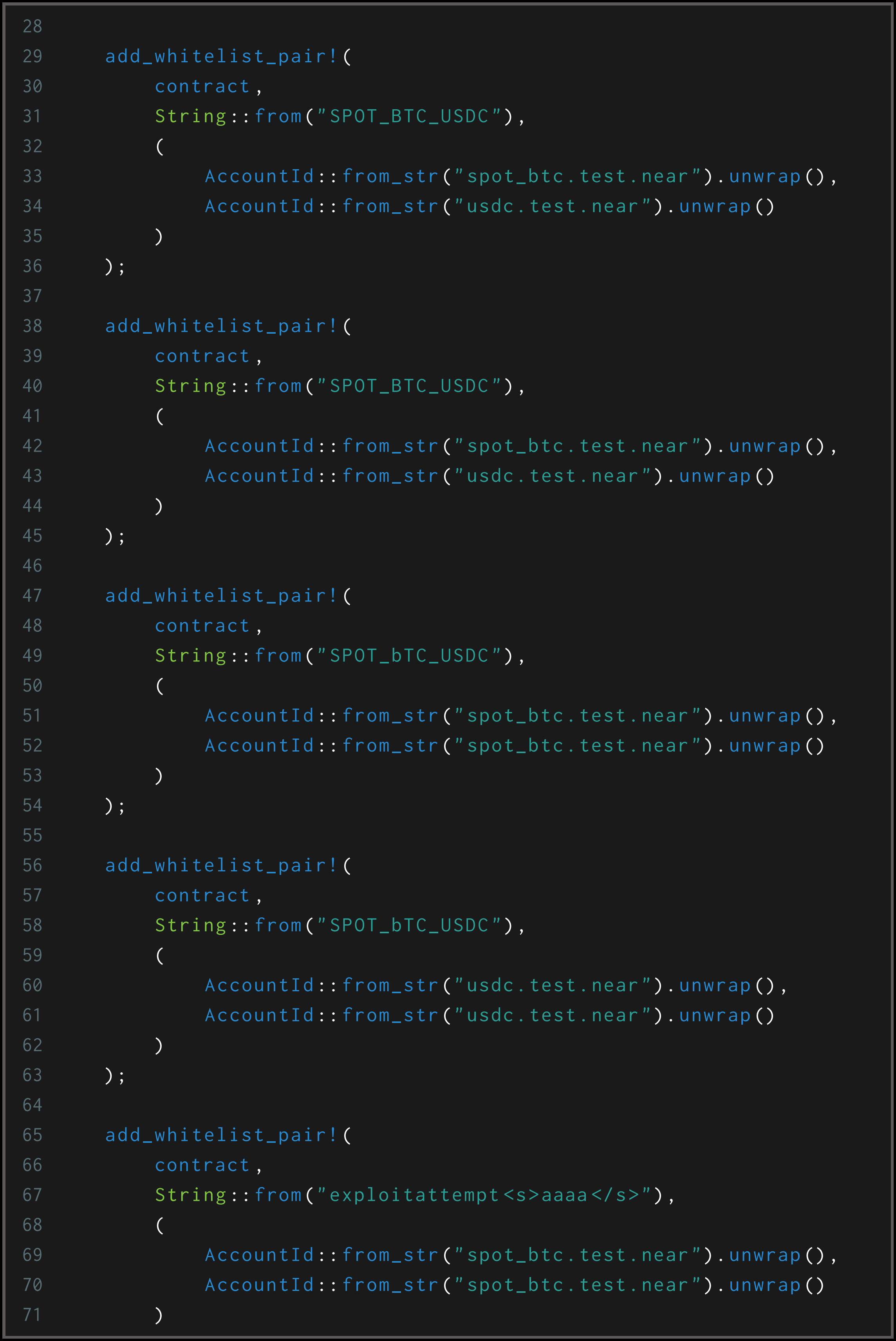
Code Location:

Listing 9: src/contract.rs (Lines 203,204)

```
197 // Add pair to the whitelist.
198     /// # Transaction panics
199     ///
200     /// * If caller is not owner
201     pub fn add_whitelist_pair(&mut self, pair_symbol: String, account_ids: (AccountId, AccountId)) {
202         self.assert_owner();
203         self.pairs_tokens_whitelist
204             .insert(&pair_symbol, &account_ids);
205     }
```

Listing 10: src/tests.rs

```

#[test]
fn pairspairs() {
    let mut contract = contract!();

    let token_id1 = "spot_btc.test.near";
    let token_id2 = "usdc.test.near";
    let fee_token = "ft-manager.test.near";

    let user_id1 = "alice";
    let user_id2 = "bob";

    create_user_account!(contract, user_id1);
    create_user_account!(contract, user_id2);

    set_token_allowed!(contract, token_id1, true);
    set_token_allowed!(contract, token_id2, true);
    set_token_allowed!(contract, fee_token, true);

    add_whitelist_pair!(
        contract,
        String::from("SPOT_BTC_USDC"),
        (
            AccountId::from_str("spot_btc.test.near").unwrap(),
            AccountId::from_str("usdc.test.near").unwrap()
        )
    );
```



```

    add_whitelist_pair!(
        contract,
        String::from("SPOT_BTC_USDC"),
        (
            AccountId::from_str("spot_btc.test.near").unwrap(),
            AccountId::from_str("usdc.test.near").unwrap()
        )
    );

    add_whitelist_pair!(
        contract,
        String::from("SPOT_BTC_USDC"),
        (
            AccountId::from_str("spot_btc.test.near").unwrap(),
            AccountId::from_str("usdc.test.near").unwrap()
        )
    );

    add_whitelist_pair!(
        contract,
        String::from("SPOT_bTC_USDC"),
        (
            AccountId::from_str("spot_btc.test.near").unwrap(),
            AccountId::from_str("spot_btc.test.near").unwrap()
        )
    );

    add_whitelist_pair!(
        contract,
        String::from("SPOT_bTC_USDC"),
        (
            AccountId::from_str("usdc.test.near").unwrap(),
            AccountId::from_str("usdc.test.near").unwrap()
        )
    );

    add_whitelist_pair!(
        contract,
        String::from("exploitattempt<s>aaaa</s>"),
        (
            AccountId::from_str("spot_btc.test.near").unwrap(),
            AccountId::from_str("spot_btc.test.near").unwrap()
        )
    );

    let pairstr = String::from("SPOT_BTC_USDC");
    println!("uppercase: {:?}\n", contract.pairs_tokens_whitelist.get(&pairstr));

    let pairstr = String::from("SPOT_bTC_USDC");
    println!("mixedcase: {:?}\n", contract.pairs_tokens_whitelist.get(&pairstr));

    let pairstr = String::from("web2exploitattempt<s>aaaa</s>");
    println!("web2exploitattempt: {:?}\n", contract.pairs_tokens_whitelist.get(&pairstr));

}

```

Risk Level:

Likelihood - 2
Impact - 5

Recommendation:

It is recommended to increase pair management security via implementing following features:

- controlling, how already existing pairs are handled (should they be overwritten as it is now?)
- considering adding remove (delisting) possibility
- validating pairs not to have double the same account IDs as members (AA pairs)
- normalizing pair name, e.g. by declining non-alphanumeric characters with is_alphanumeric and then converting the names to uppercase.

Remediation plan:

SOLVED: The issue was fixed in commit 11a5ae1594630867411141083ae86e30e80fad69a by adding additional checks on symbol format, uniqueness check, alphanumeric check and whether the symbol already exists.

3.6 (HAL-06) EXCESSIVELY CENTRALIZED FEATURES - MEDIUM

Description:

A functionality was found allowing the owner to delete key information from the contract's storage, effectively locking the funds of any user who has participated in the Orderly Protocol.

In addition to malicious actors compromising the admin account, insiders could leverage this functionality to cause griefing on their users and the organization and deleting the contract.

Normally, the contract's account shouldn't be easily deleted due to DeleteAccountWithLargeState error. However, after clearing of contract storage, this operation should be possible.

If the owner account is compromised and state is already deleted, the attacker can further potentially delete the contract, draining all NEAR balance to their wallet using NEAR's account delete feature.

Code Location:

Listing 11: src/owner.rs (Line 38)

```
38 pub fn clear_on_remove(&mut self) {
39     self.assert_owner();
40     self.user_keys.clear();
41     self.tokens_whitelist.clear();
42     self.user_token_balances.clear();
43 }
```

Risk Level:

Likelihood - 2
Impact - 5

Recommendation:

It is recommended to consider if allowing such operation on contract is needed. Moreover, it is recommended to use a multisignature wallet for sensitive accounts.

Reference:

- https://stackoverflow.com/questions/70616916/how-to-delete-near-account-with-la
- https://docs.near.org/docs/tools/near-cli#near-delete

Remediation plan:

SOLVED: The issue was fixed in commit 11a5ae159463086741141083ae86e30e80fad69a by completely removing this function.

3.7 (HAL-07) MISSING AUTHORIZATION CHECK - LOW

Description:

It was noticed that function operator_execute_match which is called by operator_execute_action does not employ authorization check like assert_contract_or_operator. The function does not contain any logic so far, so there is no impact on calling it, but it is being highlighted in order to pay attention to it in further development process, as it would allow performing actions on behalf of operator.

Code Location:

Listing 12: src/operator.rs (Lines 164-166)

```rust
161     /// Process a single operator action.
162     pub fn operator_execute_action(&mut self, action: OperatorAction) -> PromiseOrValue<()> {
163         match action {
164             OperatorAction::Execution(execution) => {
165                 self.operator_execute_match(execution);
166                 PromiseOrValue::Value(())
167             }
168             OperatorAction::Withdraw {
169                 account_id,
170                 token_id,
171             } => self.operator_withdraw_approve(account_id, token_id),
172         }
173     }
```

Listing 13: src/operator.rs (Line 182)

```rust
175     /// Execute match and update amounts on the account.
176     /// Receives two sides of the trade and how much filled.
177     ///
178     /// # Transaction panics
179     /// * Invalid signatures on the orders.
```

```
    /// * Non matching orders.
    /// * Not enough funds on the account to update after match.
    fn operator_execute_match(&mut self, _execution: Execution) {}

```

Listing 14: src/types.rs

```
pub struct Execution {
    // pair: u32,
    // taker: Order,
    // taker_signature: Signature,
    // maker: Order,
    // maker_signature: Signature,
    //
    // filled_amount: Balance,
}

```

Risk Level:

Likelihood - 1
Impact - 4

Recommendation:

It is recommended to ensure the operator_manager authorization check in further development.

Remediation plan:

SOLVED: The issue was solved in commit 11a5ae15946308674114 1083ae86e30e80fad69a : the aforementioned operation no longer exists.

3.8 (HAL-08) REDUNDANT CODE - INFORMATIONAL

Description:

It was found that some code present in the smart contract is not used. For both optimization and clearer code reasons, it is recommended to verify, if the code can be removed.

User creation already forbids the fee_collector from registering. As the user_announce_key function checks if the calling user is part of the users list, accounts that pass this check will always pass the second one.

Code Location:

Listing 15: src/contract.rs (Line 219)

```
219 if self.fee_collector == user {
220     env::panic_str("user account shouldn't be fee collector");
221 }
```

Listing 16: src/contract.rs (Line 182)

```
179 if self.users.contains(&user) {
180     env::panic_str("user account already exists");
181 }
182 if &user == &self.fee_collector {
183     env::panic_str("user could not be fee_collector");
184 }
```

Moreover, upon compilation it was noticed that some declared variables are not used, which was highlighted by the compiler:

Listing 17

```
warning: unused variable: `batch_id`
   --> src/operator.rs:304:9
    |
304 |         batch_id: i64,
    |         ^^^^^^^^ help: if this is intentional, prefix it with an underscore: `_batch_id`
    |
    = note: `#[warn(unused_variables)]` on by default

warning: unused variable: `meta`
   --> src/operator.rs:305:9
    |
305 |         meta: MetaResponse,
    |         ^^^^ help: if this is intentional, prefix it with an underscore: `_meta`

warning: `asset-manager` (lib) generated 2 warnings
```

Risk Level:

Likelihood - 1
Impact - 1

Recommendation:

Remove the fee_collector check from user_announce_key, as it is already implicit for anyone who is part of the users list. Examine if aforementioned variables should be used; otherwise, it is recommended to remove them from the contract code.

Remediation plan:

SOLVED: The issue no longer exist in commit 11a5ae15946308674114108 3ae86e30e80fad69a because the code was changed. Compilation warnings are not present now.

3.9 (HAL-09) OPERATOR KEY IS NOT DELETED ON OPERATOR CHANGE - INFORMATIONAL

Description:

When changing operator_manager, their access key held in storage is unaffected, which means the previous key will be matched to the new operator_manager. This might cause confusion or unnecessary gas expenditures until realized and changed.

Code Location:

Listing 18: src/owner.rs

```
    pub fn set_operator_manager(&mut self, operator_manager: AccountId) {
        self.assert_owner_or_operator();
        self.operator_manager = operator_manager;
    }
```

Risk Level:

Likelihood - 1
Impact - 1

Recommendation:

On changing operator_manager, any storage related solely to the old user should be cleared.

Remediation plan:

ACKNOWLEDGED: The \client team acknowledged this finding.

AUTOMATED TESTING

4.1 AUTOMATED ANALYSIS

Description:

Halborn used automated security scanners to assist with detection of well-known security issues and vulnerabilities. Among the tools used was cargo audit, a security scanner for vulnerabilities reported to the RustSec 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. 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.

ID	package	Short Description
RUSTSEC-2020-0071	time 0.1.43	Potential segfault in the time crate, upgrade to >=0.2.23

Code Location:

Listing 19: Dependency tree

```
time 0.1.43
 chrono 0.4.19
     near-primitives 0.10.0
         near-vm-logic 0.10.0
             near-sdk 4.0.0-pre.7
                 near-contract-standards 4.0.0-pre.7
                    asset-manager 0.1.0
                 asset-manager 0.1.0
```

cargo outdated

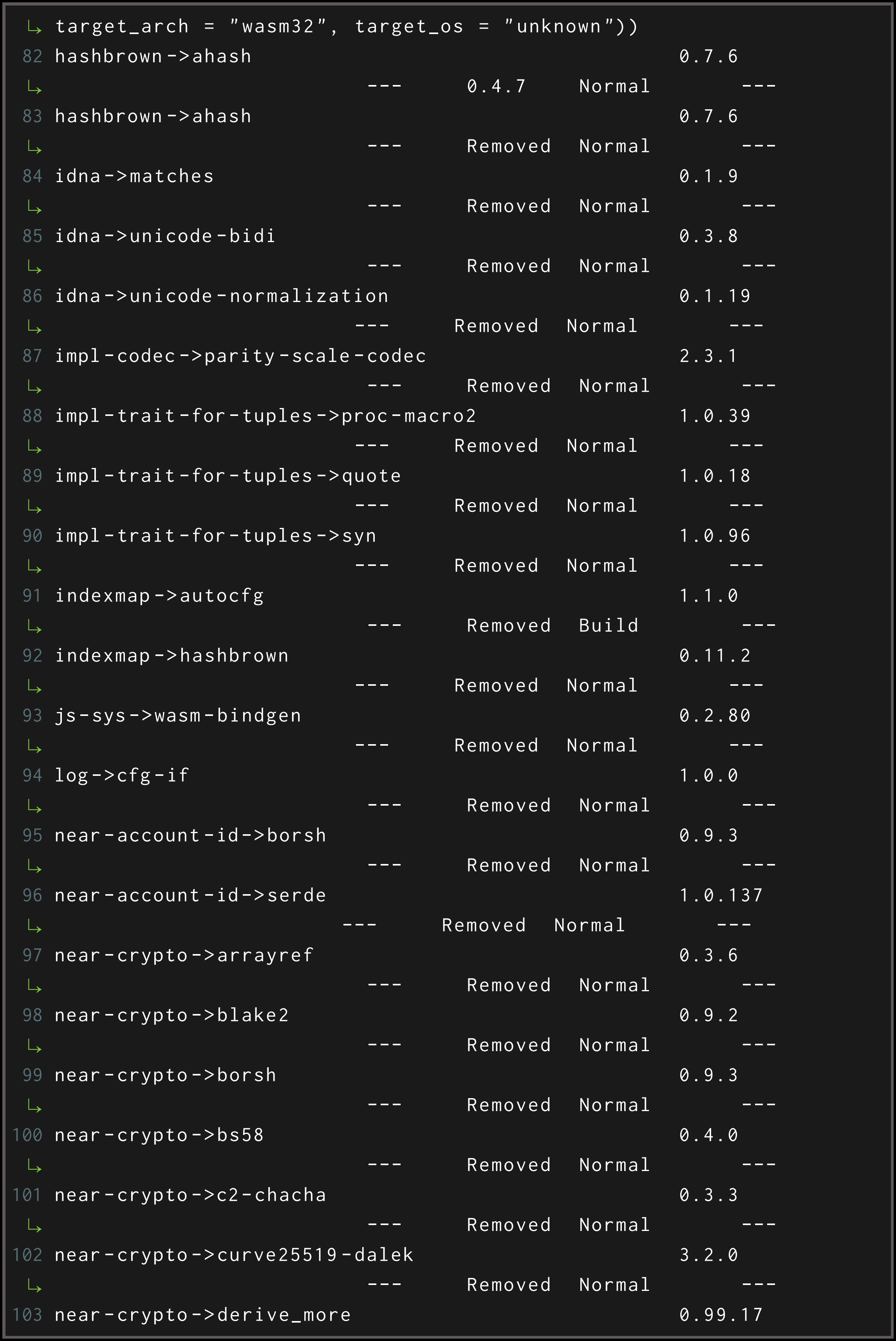
Listing 20

```
  Name                                              Project
↳                        Compat  Latest   Kind         Platform
  ----                                              -------
↳                        ------  ------   ----         ---------
  ahash->getrandom                                  0.2.6
↳                          ---     Removed  Normal       cfg(any(
↳ target_os = "linux", target_os = "android", target_os = "windows",
↳  target_os = "macos", target_os = "ios", target_os = "freebsd",
↳ target_os = "openbsd", target_os = "netbsd", target_os = "
↳ dragonfly", target_os = "solaris", target_os = "illumos",
↳ target_os = "fuchsia", target_os = "redox", target_os = "cloudabi
↳ ", target_os = "haiku", target_os = "vxworks", target_os = "
↳ emscripten", target_os = "wasi"))
  ahash->once_cell                                  1.12.0
↳                         ---     Removed  Normal       cfg(not(all(
↳ target_arch = "arm", target_os = "none")))
  ahash->version_check                              0.9.4
↳                          ---     Removed  Build        ---
  aho-corasick->memchr                              2.5.0
↳                          ---     Removed  Normal       ---
  bitvec->funty                                     1.1.0
↳                          ---     Removed  Normal       ---
  bitvec->radium                                    0.6.2
↳                          ---     Removed  Normal       ---
  bitvec->tap                                       1.0.1
↳                          ---     Removed  Normal       ---
  bitvec->wyz                                       0.2.0
↳                          ---     Removed  Normal       ---
  blake2->crypto-mac                                0.8.0
↳                          ---     Removed  Normal       ---
  blake2->digest                                    0.9.0
↳                          ---     Removed  Normal       ---
  blake2->opaque-debug                              0.3.0
↳                          ---     Removed  Normal       ---
  block-buffer->block-padding                       0.2.1
↳                          ---     Removed  Normal       ---
  block-buffer->generic-array                       0.14.5
↳                         ---     Removed  Normal       ---
  borsh->borsh-derive                               0.9.3
↳                          ---     0.8.2    Normal       ---
  borsh->borsh-derive                               0.9.3
↳                          ---     Removed  Normal       ---
  borsh->hashbrown                                  0.11.2
```

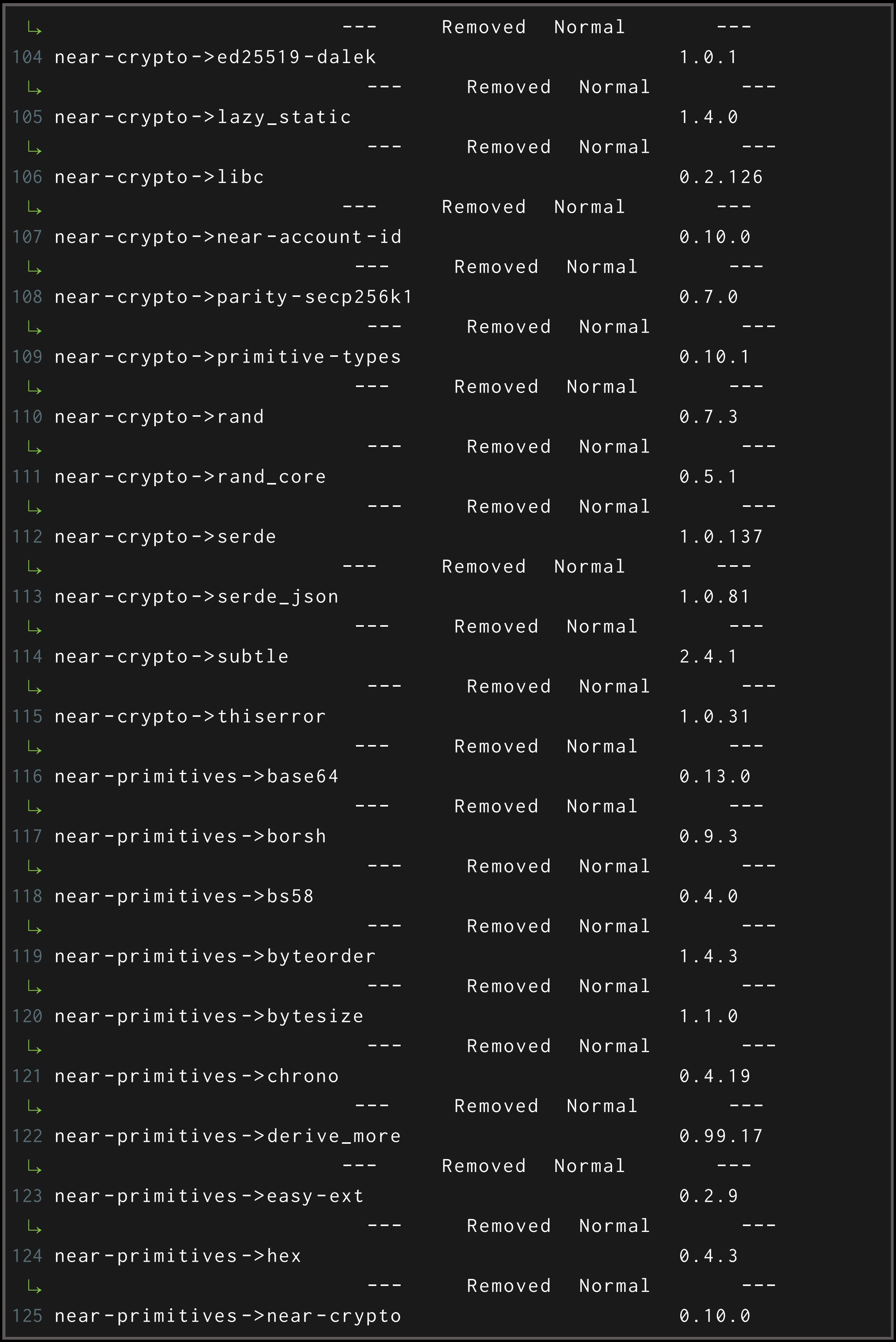
```
↳                       ---     0.9.1    Normal       ---
borsh->hashbrown                                  0.11.2
↳                       ---     Removed  Normal       ---
borsh-derive->borsh-derive-internal               0.9.3
↳                        ---     0.8.2    Normal       ---
borsh-derive->borsh-derive-internal               0.9.3
↳                        ---     Removed  Normal       ---
borsh-derive->borsh-schema-derive-internal        0.9.3
↳                        ---     0.8.2    Normal       ---
borsh-derive->borsh-schema-derive-internal        0.9.3
↳                        ---     Removed  Normal       ---
borsh-derive->proc-macro-crate                    0.1.5
↳                        ---     Removed  Normal       ---
borsh-derive->proc-macro2                         1.0.39
↳                       ---     Removed  Normal       ---
borsh-derive->syn                                 1.0.96
↳                       ---     Removed  Normal       ---
borsh-derive-internal->proc-macro2                1.0.39
↳                       ---     Removed  Normal       ---
borsh-derive-internal->quote                      1.0.18
↳                       ---     Removed  Normal       ---
borsh-derive-internal->syn                        1.0.96
↳                       ---     Removed  Normal       ---
borsh-schema-derive-internal->proc-macro2         1.0.39
↳                       ---     Removed  Normal       ---
borsh-schema-derive-internal->quote               1.0.18
↳                       ---     Removed  Normal       ---
borsh-schema-derive-internal->syn                 1.0.96
↳                       ---     Removed  Normal       ---
c2-chacha->cipher                                 0.2.5
↳                        ---     Removed  Normal       ---
c2-chacha->ppv-lite86                             0.2.16
↳                       ---     Removed  Normal       ---
chrono->libc                                      0.2.126
↳                      ---     Removed  Normal       ---
chrono->num-integer                               0.1.45
↳                       ---     Removed  Normal       ---
chrono->num-traits                                0.2.15
↳                       ---     Removed  Normal       ---
chrono->serde                                     1.0.137
↳                      ---     Removed  Normal       ---
chrono->time                                      0.1.43
↳                       ---     Removed  Normal       ---
chrono->winapi                                    0.3.9
```

```
↳                          ---     Removed   Normal       cfg(windows
↳ )
cipher->generic-array                                     0.14.5
↳                         ---     Removed   Normal       ---
cpufeatures->libc                                         0.2.126
↳                        ---     Removed   Normal       aarch64-apple
↳ -darwin
crypto-common->generic-array                              0.14.5
↳                         ---     Removed   Normal       ---
crypto-common->typenum                                    1.15.0
↳                         ---     Removed   Normal       ---
crypto-mac->generic-array                                 0.14.5
↳                         ---     Removed   Normal       ---
crypto-mac->subtle                                        2.4.1
↳                          ---     Removed   Normal       ---
curve25519-dalek->byteorder                               1.4.3
↳                          ---     Removed   Normal       ---
curve25519-dalek->digest                                  0.9.0
↳                          ---     Removed   Normal       ---
curve25519-dalek->rand_core                               0.5.1
↳                          ---     Removed   Normal       ---
curve25519-dalek->subtle                                  2.4.1
↳                          ---     Removed   Normal       ---
curve25519-dalek->zeroize                                 1.5.5
↳                          ---     Removed   Normal       ---
derive_more->convert_case                                 0.4.0
↳                          ---     Removed   Normal       ---
derive_more->proc-macro2                                  1.0.39
↳                         ---     Removed   Normal       ---
derive_more->quote                                        1.0.18
↳                         ---     Removed   Normal       ---
derive_more->rustc_version                                0.4.0
↳                          ---     Removed   Build        ---
derive_more->syn                                          1.0.96
↳                         ---     Removed   Normal       ---
digest->block-buffer                                      0.10.2
↳                         ---     Removed   Normal       ---
digest->crypto-common                                     0.1.3
↳                          ---     Removed   Normal       ---
digest->generic-array                                     0.14.5
↳                         ---     Removed   Normal       ---
digest->subtle                                            2.4.1
↳                          ---     Removed   Normal       ---
ed25519->signature                                        1.5.0
```

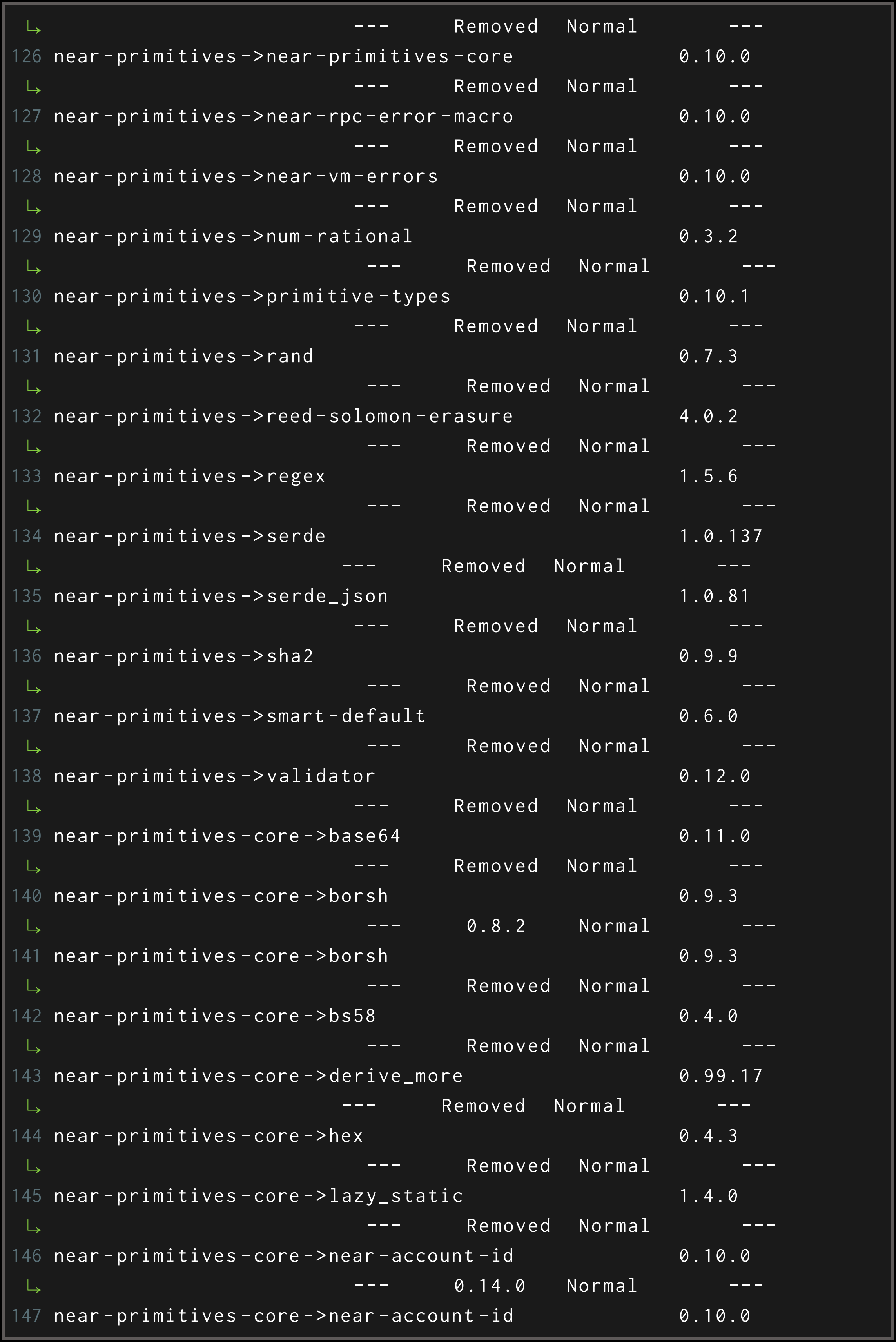
```
↳                          ---     Removed  Normal       ---
ed25519-dalek->curve25519-dalek                     3.2.0
↳                          ---     Removed  Normal       ---
ed25519-dalek->ed25519                              1.5.2
↳                          ---     Removed  Normal       ---
ed25519-dalek->rand                                 0.7.3
↳                          ---     Removed  Normal       ---
ed25519-dalek->serde                                1.0.137
↳                        ---     Removed  Normal       ---
ed25519-dalek->sha2                                 0.9.9
↳                          ---     Removed  Normal       ---
ed25519-dalek->zeroize                              1.5.5
↳                          ---     Removed  Normal       ---
fixed-hash->byteorder                               1.4.3
↳                          ---     Removed  Normal       ---
fixed-hash->rand                                    0.8.5
↳                          ---     Removed  Normal       ---
fixed-hash->rustc-hex                               2.1.0
↳                          ---     Removed  Normal       ---
fixed-hash->static_assertions                       1.1.0
↳                          ---     Removed  Normal       ---
form_urlencoded->matches                            0.1.9
↳                          ---     Removed  Normal       ---
form_urlencoded->percent-encoding                   2.1.0
↳                          ---     Removed  Normal       ---
generic-array->typenum                              1.15.0
↳                         ---     Removed  Normal       ---
generic-array->version_check                        0.9.4
↳                          ---     Removed  Build        ---
getrandom->cfg-if                                   1.0.0
↳                          ---     Removed  Normal       ---
getrandom->js-sys                                   0.3.57
↳                         ---     Removed  Normal       cfg(all(
↳ target_arch = "wasm32", target_os = "unknown"))
getrandom->libc                                     0.2.126
↳                        ---     Removed  Normal       cfg(unix)
getrandom->wasi                                     0.10.2+wasi-
↳ snapshot-preview1  ---     Removed  Normal      cfg(target_os = "
↳ wasi")
getrandom->wasi                                     0.9.0+wasi-
↳ snapshot-preview1   ---     Removed  Normal       cfg(target_os =
↳ "wasi")
getrandom->wasm-bindgen                             0.2.80
↳                         ---     Removed  Normal       cfg(all(
```



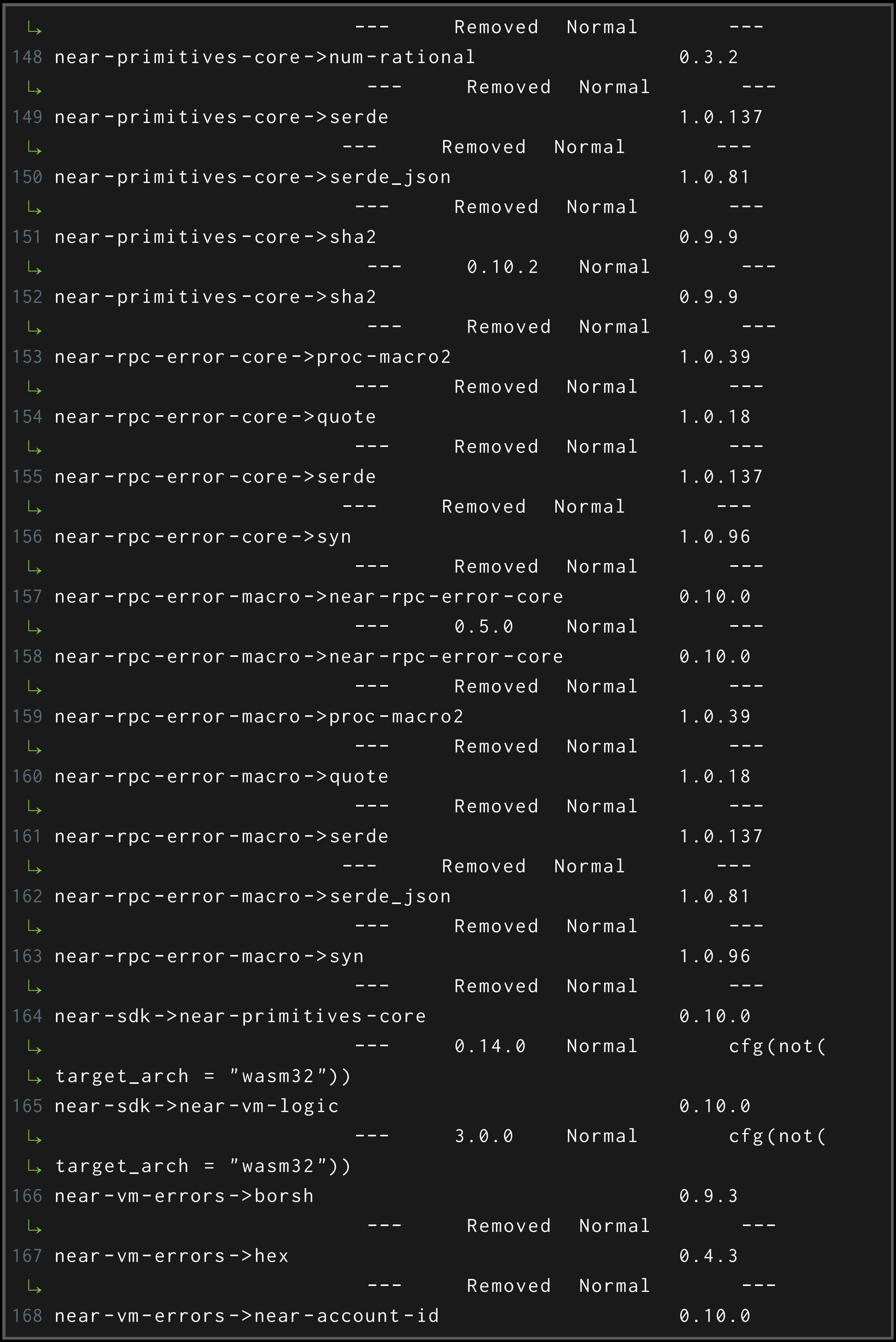
```
↳ target_arch = "wasm32", target_os = "unknown"))
hashbrown->ahash                                   0.7.6
↳                         ---     0.4.7    Normal       ---
hashbrown->ahash                                   0.7.6
↳                         ---     Removed  Normal       ---
idna->matches                                      0.1.9
↳                         ---     Removed  Normal       ---
idna->unicode-bidi                                 0.3.8
↳                         ---     Removed  Normal       ---
idna->unicode-normalization                        0.1.19
↳                        ---     Removed  Normal       ---
impl-codec->parity-scale-codec                     2.3.1
↳                         ---     Removed  Normal       ---
impl-trait-for-tuples->proc-macro2                 1.0.39
↳                        ---     Removed  Normal       ---
impl-trait-for-tuples->quote                       1.0.18
↳                        ---     Removed  Normal       ---
impl-trait-for-tuples->syn                         1.0.96
↳                        ---     Removed  Normal       ---
indexmap->autocfg                                  1.1.0
↳                         ---     Removed  Build        ---
indexmap->hashbrown                                0.11.2
↳                        ---     Removed  Normal       ---
js-sys->wasm-bindgen                               0.2.80
↳                        ---     Removed  Normal       ---
log->cfg-if                                        1.0.0
↳                         ---     Removed  Normal       ---
near-account-id->borsh                             0.9.3
↳                         ---     Removed  Normal       ---
near-account-id->serde                             1.0.137
↳                       ---     Removed  Normal       ---
near-crypto->arrayref                              0.3.6
↳                         ---     Removed  Normal       ---
near-crypto->blake2                                0.9.2
↳                         ---     Removed  Normal       ---
near-crypto->borsh                                 0.9.3
↳                         ---     Removed  Normal       ---
near-crypto->bs58                                  0.4.0
↳                         ---     Removed  Normal       ---
near-crypto->c2-chacha                             0.3.3
↳                         ---     Removed  Normal       ---
near-crypto->curve25519-dalek                      3.2.0
↳                         ---     Removed  Normal       ---
near-crypto->derive_more                           0.99.17
```



```
↳                        ---     Removed   Normal       ---
  near-crypto->ed25519-dalek                        1.0.1
↳                          ---     Removed   Normal       ---
  near-crypto->lazy_static                          1.4.0
↳                          ---     Removed   Normal       ---
  near-crypto->libc                                 0.2.126
↳                        ---     Removed   Normal       ---
  near-crypto->near-account-id                      0.10.0
↳                         ---     Removed   Normal       ---
  near-crypto->parity-secp256k1                     0.7.0
↳                          ---     Removed   Normal       ---
  near-crypto->primitive-types                      0.10.1
↳                         ---     Removed   Normal       ---
  near-crypto->rand                                 0.7.3
↳                          ---     Removed   Normal       ---
  near-crypto->rand_core                            0.5.1
↳                          ---     Removed   Normal       ---
  near-crypto->serde                                1.0.137
↳                        ---     Removed   Normal       ---
  near-crypto->serde_json                           1.0.81
↳                         ---     Removed   Normal       ---
  near-crypto->subtle                               2.4.1
↳                          ---     Removed   Normal       ---
  near-crypto->thiserror                            1.0.31
↳                         ---     Removed   Normal       ---
  near-primitives->base64                           0.13.0
↳                         ---     Removed   Normal       ---
  near-primitives->borsh                            0.9.3
↳                          ---     Removed   Normal       ---
  near-primitives->bs58                             0.4.0
↳                          ---     Removed   Normal       ---
  near-primitives->byteorder                        1.4.3
↳                          ---     Removed   Normal       ---
  near-primitives->bytesize                         1.1.0
↳                          ---     Removed   Normal       ---
  near-primitives->chrono                           0.4.19
↳                         ---     Removed   Normal       ---
  near-primitives->derive_more                      0.99.17
↳                        ---     Removed   Normal       ---
  near-primitives->easy-ext                         0.2.9
↳                          ---     Removed   Normal       ---
  near-primitives->hex                              0.4.3
↳                          ---     Removed   Normal       ---
  near-primitives->near-crypto                      0.10.0
```

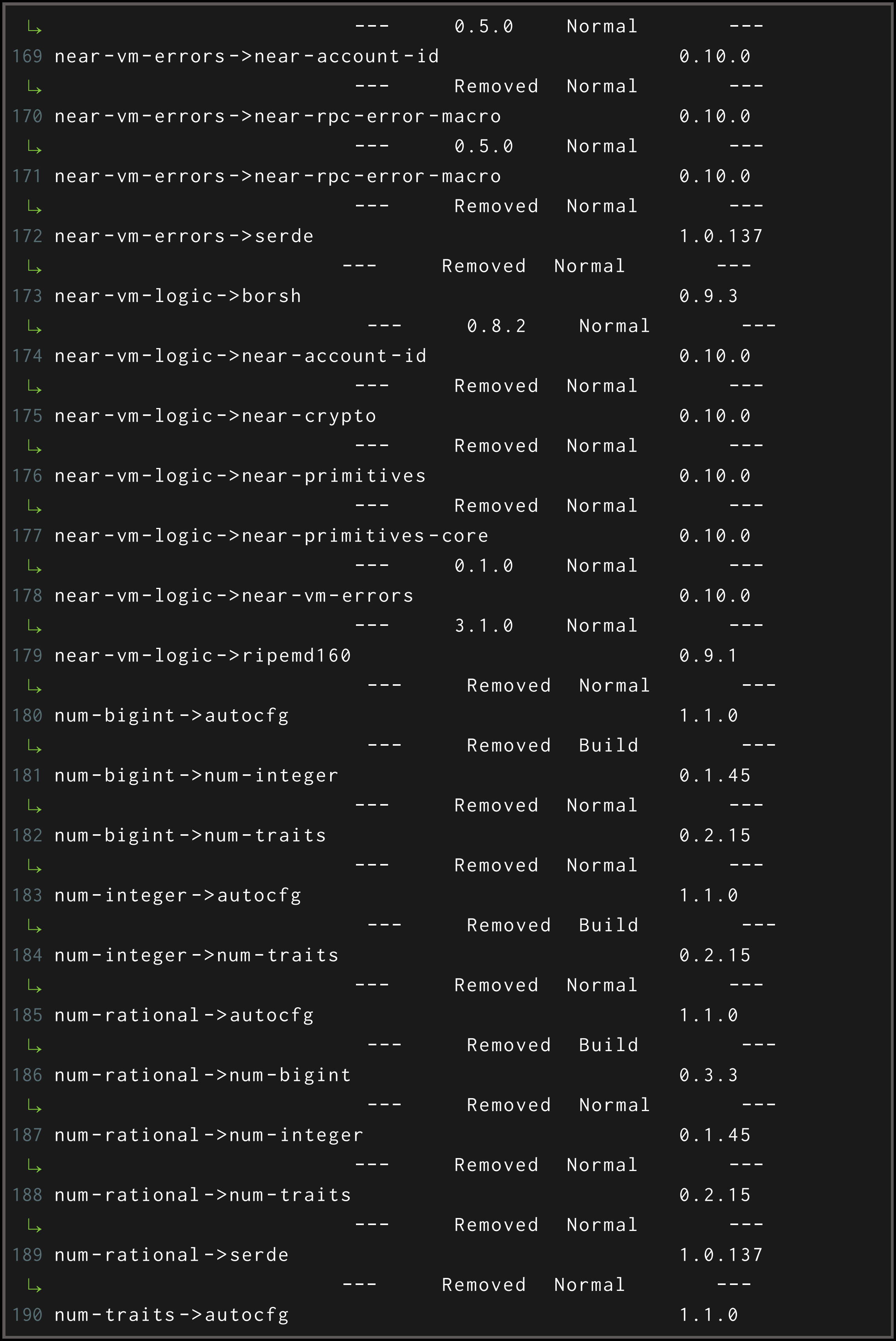


```
↳                       ---     Removed  Normal       ---
near-primitives->near-primitives-core             0.10.0
↳                       ---     Removed  Normal       ---
near-primitives->near-rpc-error-macro             0.10.0
↳                       ---     Removed  Normal       ---
near-primitives->near-vm-errors                   0.10.0
↳                       ---     Removed  Normal       ---
near-primitives->num-rational                     0.3.2
↳                        ---     Removed  Normal       ---
near-primitives->primitive-types                  0.10.1
↳                       ---     Removed  Normal       ---
near-primitives->rand                             0.7.3
↳                        ---     Removed  Normal       ---
near-primitives->reed-solomon-erasure             4.0.2
↳                        ---     Removed  Normal       ---
near-primitives->regex                            1.5.6
↳                        ---     Removed  Normal       ---
near-primitives->serde                            1.0.137
↳                      ---     Removed  Normal       ---
near-primitives->serde_json                       1.0.81
↳                       ---     Removed  Normal       ---
near-primitives->sha2                             0.9.9
↳                        ---     Removed  Normal       ---
near-primitives->smart-default                    0.6.0
↳                        ---     Removed  Normal       ---
near-primitives->validator                        0.12.0
↳                       ---     Removed  Normal       ---
near-primitives-core->base64                      0.11.0
↳                       ---     Removed  Normal       ---
near-primitives-core->borsh                       0.9.3
↳                        ---     0.8.2    Normal       ---
near-primitives-core->borsh                       0.9.3
↳                        ---     Removed  Normal       ---
near-primitives-core->bs58                        0.4.0
↳                        ---     Removed  Normal       ---
near-primitives-core->derive_more                 0.99.17
↳                      ---     Removed  Normal       ---
near-primitives-core->hex                         0.4.3
↳                        ---     Removed  Normal       ---
near-primitives-core->lazy_static                 1.4.0
↳                        ---     Removed  Normal       ---
near-primitives-core->near-account-id             0.10.0
↳                       ---     0.14.0   Normal       ---
near-primitives-core->near-account-id             0.10.0
```

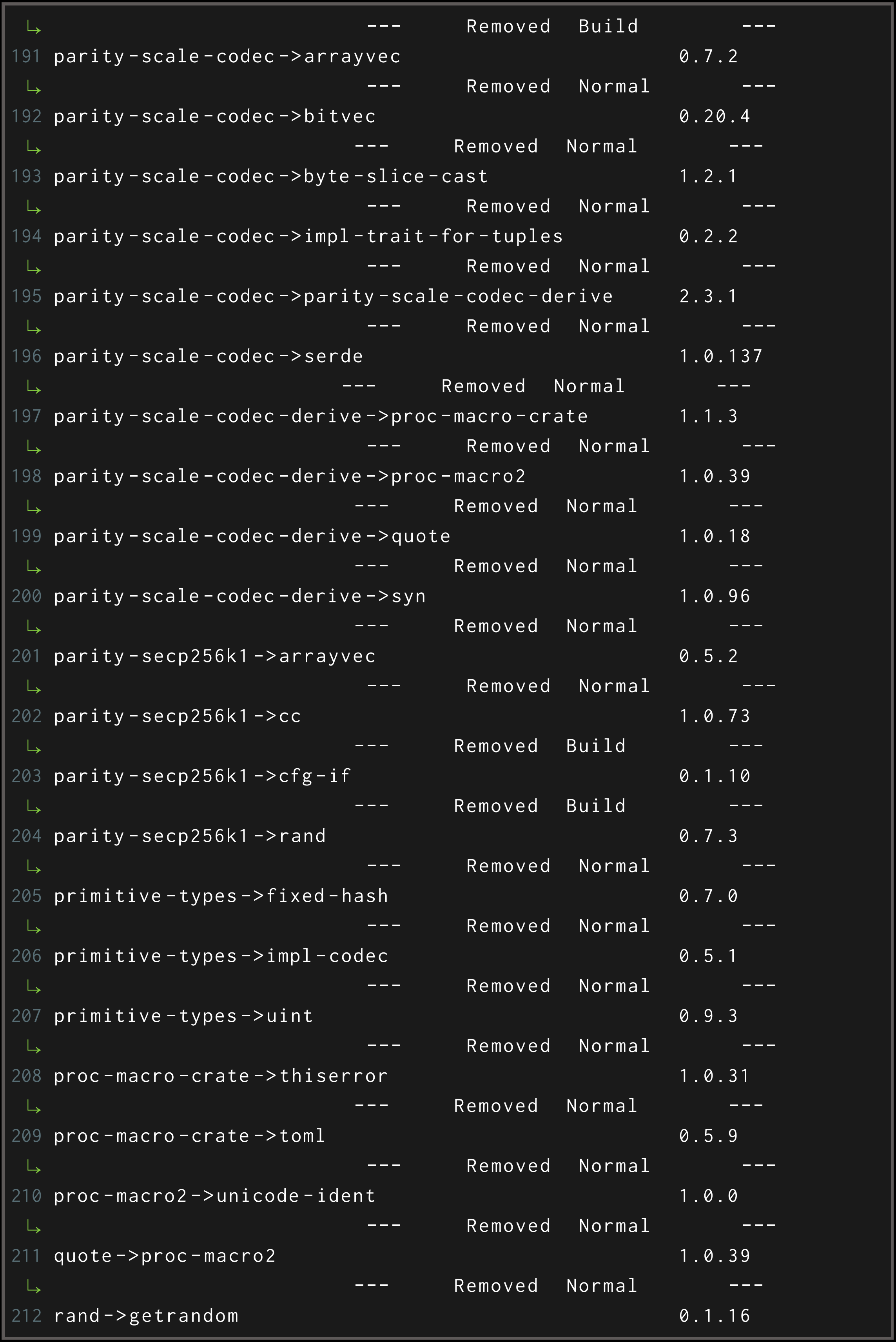


```
↳                        ---      Removed   Normal        ---
near-primitives-core->num-rational                 0.3.2
↳                         ---      Removed   Normal        ---
near-primitives-core->serde                        1.0.137
↳                       ---      Removed   Normal        ---
near-primitives-core->serde_json                   1.0.81
↳                        ---      Removed   Normal        ---
near-primitives-core->sha2                         0.9.9
↳                         ---      0.10.2    Normal        ---
near-primitives-core->sha2                         0.9.9
↳                         ---      Removed   Normal        ---
near-rpc-error-core->proc-macro2                   1.0.39
↳                        ---      Removed   Normal        ---
near-rpc-error-core->quote                         1.0.18
↳                        ---      Removed   Normal        ---
near-rpc-error-core->serde                         1.0.137
↳                       ---      Removed   Normal        ---
near-rpc-error-core->syn                           1.0.96
↳                        ---      Removed   Normal        ---
near-rpc-error-macro->near-rpc-error-core          0.10.0
↳                        ---      0.5.0     Normal        ---
near-rpc-error-macro->near-rpc-error-core          0.10.0
↳                        ---      Removed   Normal        ---
near-rpc-error-macro->proc-macro2                  1.0.39
↳                        ---      Removed   Normal        ---
near-rpc-error-macro->quote                        1.0.18
↳                        ---      Removed   Normal        ---
near-rpc-error-macro->serde                        1.0.137
↳                       ---      Removed   Normal        ---
near-rpc-error-macro->serde_json                   1.0.81
↳                        ---      Removed   Normal        ---
near-rpc-error-macro->syn                          1.0.96
↳                        ---      Removed   Normal        ---
near-sdk->near-primitives-core                     0.10.0
↳                        ---      0.14.0    Normal        cfg(not(
↳ target_arch = "wasm32"))
near-sdk->near-vm-logic                            0.10.0
↳                        ---      3.0.0     Normal        cfg(not(
↳ target_arch = "wasm32"))
near-vm-errors->borsh                              0.9.3
↳                         ---      Removed   Normal        ---
near-vm-errors->hex                                0.4.3
↳                         ---      Removed   Normal        ---
near-vm-errors->near-account-id                    0.10.0
```

AUTOMATED TESTING



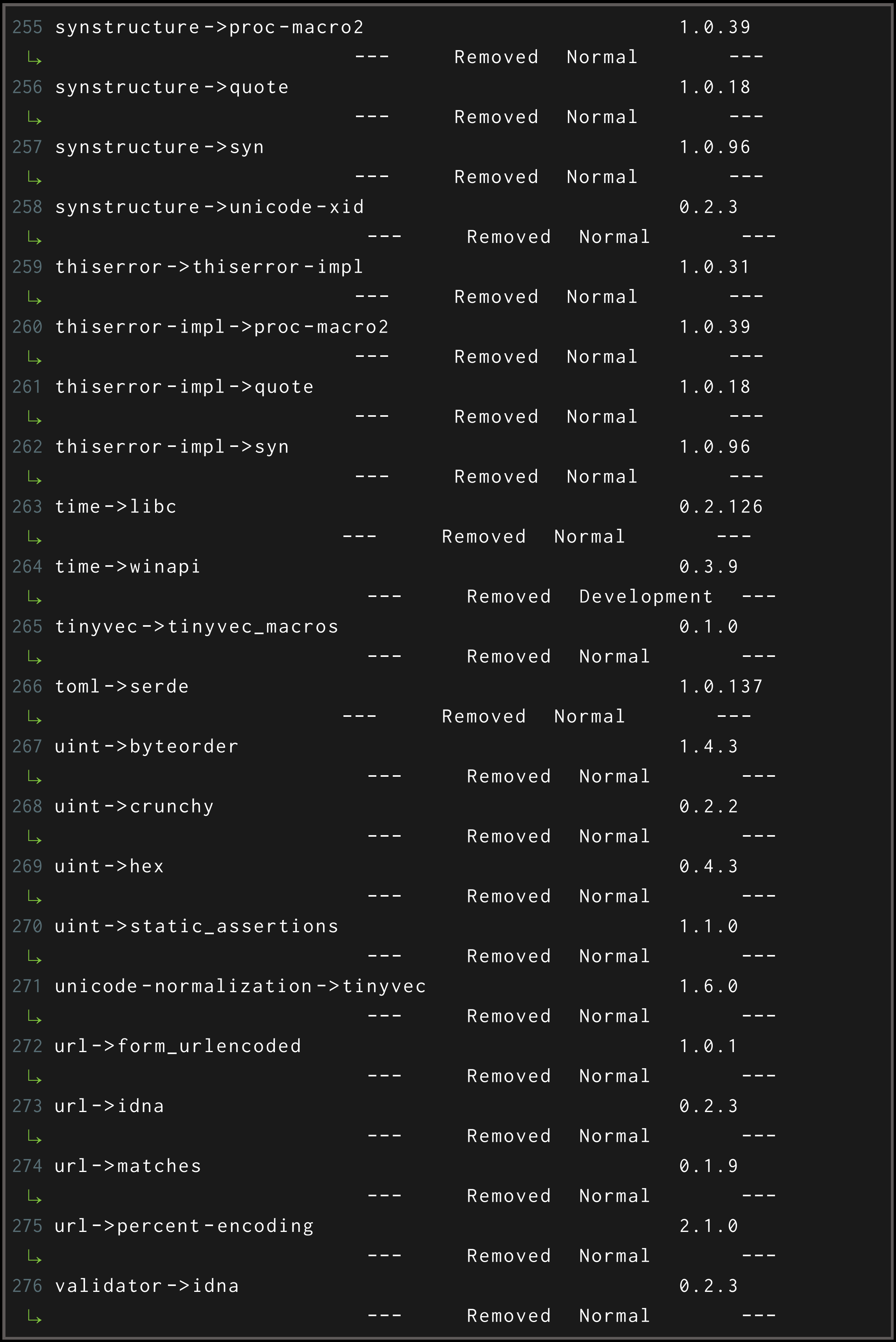
```
 ↳                        ---      0.5.0     Normal        ---
near-vm-errors->near-account-id                          0.10.0
 ↳                        ---      Removed   Normal        ---
near-vm-errors->near-rpc-error-macro                     0.10.0
 ↳                        ---      0.5.0     Normal        ---
near-vm-errors->near-rpc-error-macro                     0.10.0
 ↳                        ---      Removed   Normal        ---
near-vm-errors->serde                                    1.0.137
 ↳                       ---      Removed   Normal        ---
near-vm-logic->borsh                                     0.9.3
 ↳                         ---      0.8.2     Normal        ---
near-vm-logic->near-account-id                           0.10.0
 ↳                        ---      Removed   Normal        ---
near-vm-logic->near-crypto                               0.10.0
 ↳                        ---      Removed   Normal        ---
near-vm-logic->near-primitives                           0.10.0
 ↳                        ---      Removed   Normal        ---
near-vm-logic->near-primitives-core                      0.10.0
 ↳                        ---      0.1.0     Normal        ---
near-vm-logic->near-vm-errors                            0.10.0
 ↳                        ---      3.1.0     Normal        ---
near-vm-logic->ripemd160                                 0.9.1
 ↳                         ---      Removed   Normal        ---
num-bigint->autocfg                                      1.1.0
 ↳                         ---      Removed   Build         ---
num-bigint->num-integer                                  0.1.45
 ↳                        ---      Removed   Normal        ---
num-bigint->num-traits                                   0.2.15
 ↳                        ---      Removed   Normal        ---
num-integer->autocfg                                     1.1.0
 ↳                         ---      Removed   Build         ---
num-integer->num-traits                                  0.2.15
 ↳                        ---      Removed   Normal        ---
num-rational->autocfg                                    1.1.0
 ↳                         ---      Removed   Build         ---
num-rational->num-bigint                                 0.3.3
 ↳                         ---      Removed   Normal        ---
num-rational->num-integer                                0.1.45
 ↳                        ---      Removed   Normal        ---
num-rational->num-traits                                 0.2.15
 ↳                        ---      Removed   Normal        ---
num-rational->serde                                      1.0.137
 ↳                       ---      Removed   Normal        ---
num-traits->autocfg                                      1.1.0
```



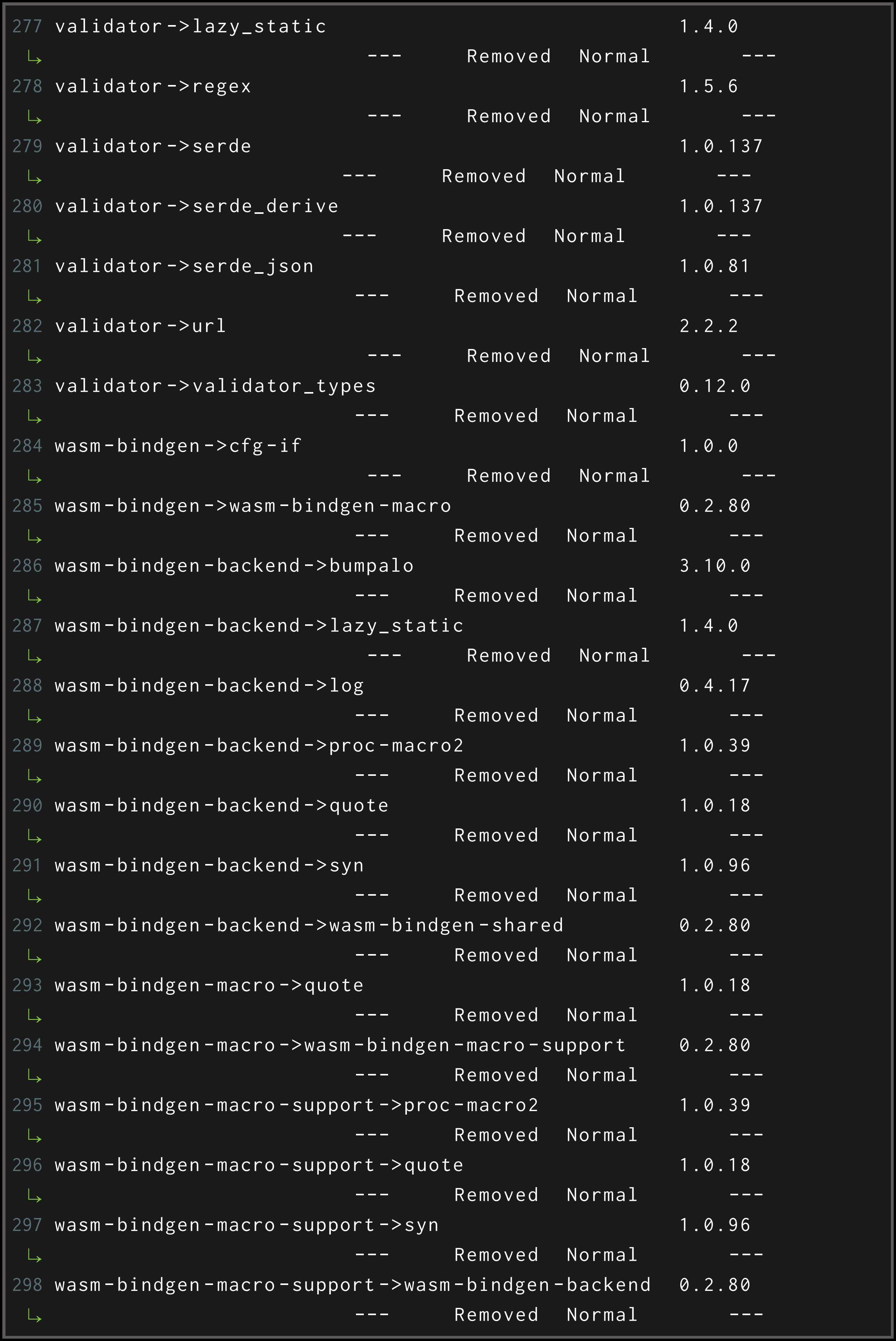
```
↳                         ---      Removed   Build        ---
parity-scale-codec->arrayvec                           0.7.2
↳                         ---      Removed   Normal       ---
parity-scale-codec->bitvec                             0.20.4
↳                        ---      Removed   Normal       ---
parity-scale-codec->byte-slice-cast                    1.2.1
↳                         ---      Removed   Normal       ---
parity-scale-codec->impl-trait-for-tuples              0.2.2
↳                         ---      Removed   Normal       ---
parity-scale-codec->parity-scale-codec-derive          2.3.1
↳                         ---      Removed   Normal       ---
parity-scale-codec->serde                              1.0.137
↳                       ---      Removed   Normal       ---
parity-scale-codec-derive->proc-macro-crate            1.1.3
↳                         ---      Removed   Normal       ---
parity-scale-codec-derive->proc-macro2                 1.0.39
↳                        ---      Removed   Normal       ---
parity-scale-codec-derive->quote                       1.0.18
↳                        ---      Removed   Normal       ---
parity-scale-codec-derive->syn                         1.0.96
↳                        ---      Removed   Normal       ---
parity-secp256k1->arrayvec                             0.5.2
↳                         ---      Removed   Normal       ---
parity-secp256k1->cc                                   1.0.73
↳                        ---      Removed   Build        ---
parity-secp256k1->cfg-if                               0.1.10
↳                        ---      Removed   Build        ---
parity-secp256k1->rand                                 0.7.3
↳                         ---      Removed   Normal       ---
primitive-types->fixed-hash                            0.7.0
↳                         ---      Removed   Normal       ---
primitive-types->impl-codec                            0.5.1
↳                         ---      Removed   Normal       ---
primitive-types->uint                                  0.9.3
↳                         ---      Removed   Normal       ---
proc-macro-crate->thiserror                            1.0.31
↳                        ---      Removed   Normal       ---
proc-macro-crate->toml                                 0.5.9
↳                         ---      Removed   Normal       ---
proc-macro2->unicode-ident                             1.0.0
↳                         ---      Removed   Normal       ---
quote->proc-macro2                                     1.0.39
↳                        ---      Removed   Normal       ---
rand->getrandom                                        0.1.16
```

```
↳                        ---      Removed   Normal        ---
rand->libc                                            0.2.126
↳                       ---      Removed   Normal        cfg(unix)
rand->rand_chacha                                     0.2.2
↳                         ---      Removed   Normal        cfg(not(
↳ target_os = "emscripten"))
rand->rand_chacha                                     0.3.1
↳                         ---      Removed   Normal        ---
rand->rand_core                                       0.5.1
↳                         ---      Removed   Normal        ---
rand->rand_core                                       0.6.3
↳                         ---      Removed   Normal        ---
rand->rand_hc                                         0.2.0
↳                         ---      Removed   Development   ---
rand_chacha->ppv-lite86                               0.2.16
↳                        ---      Removed   Normal        ---
rand_chacha->rand_core                                0.5.1
↳                         ---      Removed   Normal        ---
rand_chacha->rand_core                                0.6.3
↳                         ---      Removed   Normal        ---
rand_core->getrandom                                  0.1.16
↳                        ---      Removed   Normal        ---
rand_core->getrandom                                  0.2.6
↳                         ---      Removed   Normal        ---
rand_hc->rand_core                                    0.5.1
↳                         ---      Removed   Normal        ---
reed-solomon-erasure->smallvec                        1.8.0
↳                         ---      Removed   Normal        ---
regex->aho-corasick                                   0.7.18
↳                        ---      Removed   Normal        ---
regex->memchr                                         2.5.0
↳                         ---      Removed   Normal        ---
regex->regex-syntax                                   0.6.26
↳                        ---      Removed   Normal        ---
ripemd160->block-buffer                               0.9.0
↳                         ---      Removed   Normal        ---
ripemd160->digest                                     0.9.0
↳                         ---      Removed   Normal        ---
ripemd160->opaque-debug                               0.3.0
↳                         ---      Removed   Normal        ---
rustc_version->semver                                 1.0.9
↳                         ---      Removed   Normal        ---
serde->serde_derive                                   1.0.137
↳                       ---      Removed   Normal        ---
```

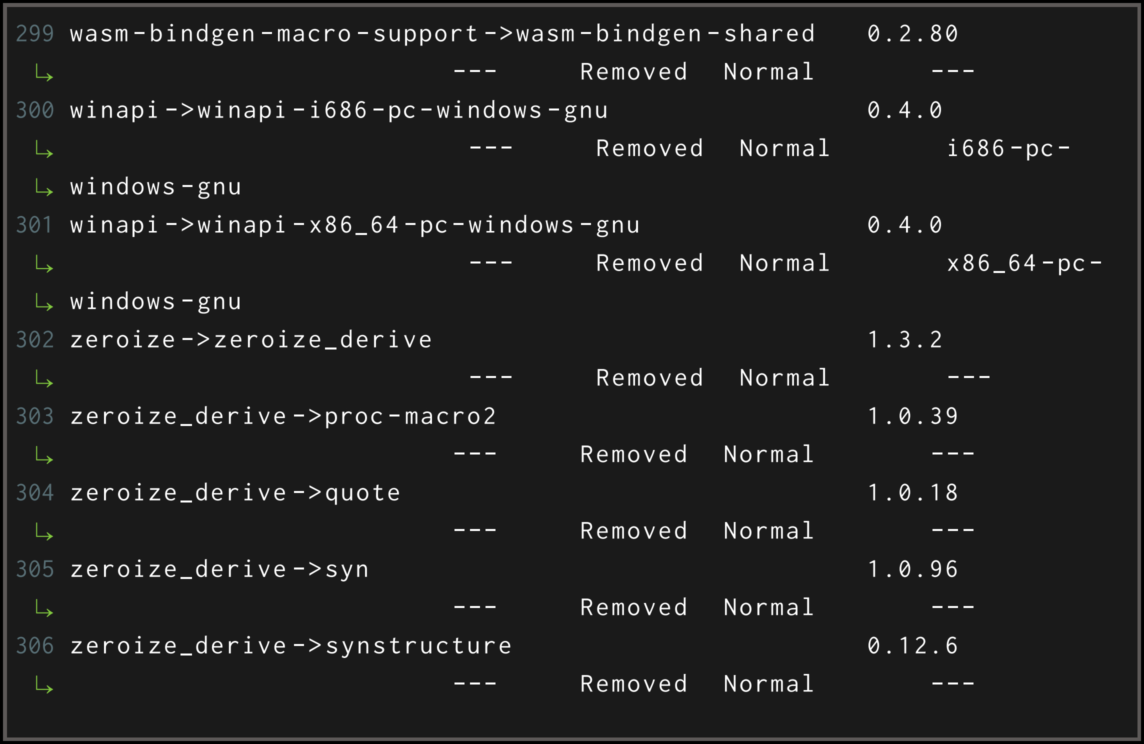
```
  serde_derive->proc-macro2                         1.0.39
↳                         ---     Removed   Normal        ---
  serde_derive->quote                               1.0.18
↳                         ---     Removed   Normal        ---
  serde_derive->syn                                 1.0.96
↳                         ---     Removed   Normal        ---
  serde_json->indexmap                              1.8.2
↳                          ---     Removed   Normal        ---
  serde_json->itoa                                  1.0.2
↳                          ---     Removed   Normal        ---
  serde_json->ryu                                   1.0.10
↳                         ---     Removed   Normal        ---
  serde_json->serde                                 1.0.137
↳                        ---     Removed   Normal        ---
  sha2->block-buffer                                0.9.0
↳                          ---     Removed   Normal        ---
  sha2->cfg-if                                      1.0.0
↳                          ---     Removed   Normal        ---
  sha2->cpufeatures                                 0.2.2
↳                          ---     Removed   Normal        cfg(any(
↳ target_arch = "aarch64", target_arch = "x86_64", target_arch = "
↳ x86"))
  sha2->digest                                      0.9.0
↳                          ---     0.10.3    Normal        ---
  sha2->digest                                      0.9.0
↳                          ---     Removed   Normal        ---
  sha2->opaque-debug                                0.3.0
↳                          ---     Removed   Normal        ---
  signature->digest                                 0.10.3
↳                         ---     Removed   Normal        ---
  signature->rand_core                              0.6.3
↳                          ---     Removed   Normal        ---
  smart-default->proc-macro2                        1.0.39
↳                         ---     Removed   Normal        ---
  smart-default->quote                              1.0.18
↳                         ---     Removed   Normal        ---
  smart-default->syn                                1.0.96
↳                         ---     Removed   Normal        ---
  syn->proc-macro2                                  1.0.39
↳                         ---     Removed   Normal        ---
  syn->quote                                        1.0.18
↳                         ---     Removed   Normal        ---
  syn->unicode-ident                                1.0.0
↳                          ---     Removed   Normal        ---
```



```
  synstructure->proc-macro2                         1.0.39
↳                         ---     Removed  Normal       ---
  synstructure->quote                               1.0.18
↳                         ---     Removed  Normal       ---
  synstructure->syn                                 1.0.96
↳                         ---     Removed  Normal       ---
  synstructure->unicode-xid                         0.2.3
↳                          ---     Removed  Normal       ---
  thiserror->thiserror-impl                         1.0.31
↳                         ---     Removed  Normal       ---
  thiserror-impl->proc-macro2                       1.0.39
↳                         ---     Removed  Normal       ---
  thiserror-impl->quote                             1.0.18
↳                         ---     Removed  Normal       ---
  thiserror-impl->syn                               1.0.96
↳                         ---     Removed  Normal       ---
  time->libc                                        0.2.126
↳                        ---     Removed  Normal       ---
  time->winapi                                      0.3.9
↳                          ---     Removed  Development  ---
  tinyvec->tinyvec_macros                           0.1.0
↳                          ---     Removed  Normal       ---
  toml->serde                                       1.0.137
↳                        ---     Removed  Normal       ---
  uint->byteorder                                   1.4.3
↳                          ---     Removed  Normal       ---
  uint->crunchy                                     0.2.2
↳                          ---     Removed  Normal       ---
  uint->hex                                         0.4.3
↳                          ---     Removed  Normal       ---
  uint->static_assertions                           1.1.0
↳                          ---     Removed  Normal       ---
  unicode-normalization->tinyvec                    1.6.0
↳                          ---     Removed  Normal       ---
  url->form_urlencoded                              1.0.1
↳                          ---     Removed  Normal       ---
  url->idna                                         0.2.3
↳                          ---     Removed  Normal       ---
  url->matches                                      0.1.9
↳                          ---     Removed  Normal       ---
  url->percent-encoding                             2.1.0
↳                          ---     Removed  Normal       ---
  validator->idna                                   0.2.3
↳                          ---     Removed  Normal       ---
```



```
validator->lazy_static                                 1.4.0
 ↳                          ---      Removed   Normal       ---
validator->regex                                       1.5.6
 ↳                          ---      Removed   Normal       ---
validator->serde                                       1.0.137
 ↳                        ---      Removed   Normal       ---
validator->serde_derive                                1.0.137
 ↳                        ---      Removed   Normal       ---
validator->serde_json                                  1.0.81
 ↳                         ---      Removed   Normal       ---
validator->url                                         2.2.2
 ↳                          ---      Removed   Normal       ---
validator->validator_types                             0.12.0
 ↳                         ---      Removed   Normal       ---
wasm-bindgen->cfg-if                                   1.0.0
 ↳                          ---      Removed   Normal       ---
wasm-bindgen->wasm-bindgen-macro                       0.2.80
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->bumpalo                          3.10.0
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->lazy_static                      1.4.0
 ↳                          ---      Removed   Normal       ---
wasm-bindgen-backend->log                              0.4.17
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->proc-macro2                      1.0.39
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->quote                            1.0.18
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->syn                              1.0.96
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-backend->wasm-bindgen-shared              0.2.80
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro->quote                              1.0.18
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro->wasm-bindgen-macro-support         0.2.80
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro-support->proc-macro2                1.0.39
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro-support->quote                      1.0.18
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro-support->syn                        1.0.96
 ↳                         ---      Removed   Normal       ---
wasm-bindgen-macro-support->wasm-bindgen-backend       0.2.80
 ↳                         ---      Removed   Normal       ---
```



```
wasm-bindgen-macro-support->wasm-bindgen-shared    0.2.80
 ↳                        ---      Removed   Normal        ---
winapi->winapi-i686-pc-windows-gnu                 0.4.0
 ↳                         ---      Removed   Normal        i686-pc-
 ↳ windows-gnu
winapi->winapi-x86_64-pc-windows-gnu               0.4.0
 ↳                         ---      Removed   Normal        x86_64-pc-
 ↳ windows-gnu
zeroize->zeroize_derive                            1.3.2
 ↳                         ---      Removed   Normal         ---
zeroize_derive->proc-macro2                        1.0.39
 ↳                        ---      Removed   Normal        ---
zeroize_derive->quote                              1.0.18
 ↳                        ---      Removed   Normal        ---
zeroize_derive->syn                                1.0.96
 ↳                        ---      Removed   Normal        ---
zeroize_derive->synstructure                       0.12.6
 ↳                        ---      Removed   Normal        ---
```

Risk Level:

Likelihood - 1
Impact - 1

Recommendation:

Beware of using dependencies and packages that are no longer supported by developers or have publicly known security flaws, even when they are not currently exploitable.

THANK YOU FOR CHOOSING

HALBORN