

Guvenkaya® The Bedrock of Security

Aurora

NEAR Intents Security Review

Contents

About Us	01
About Aurora	01
Audit Results	02
.1 Project Scope	02
.2 Out of Scope	10
.3 Timeline	10
Methodology	11
Severity Breakdown	12
.1 Likelihood Ratings	12
.2 Impact	12
.3 Severity Ratings	12
.4 Likelihood Matrix	13
.5 Likelihood/Impact Matrix	13
Findings Summary	14
Findings Details	16
.1 GUV-1 Potential Funds Stealing From Users Via Repeating Failed Intents - Medium	16
.2 GUV-2 Possible DoS Of Public Keys Viewing Per User - Low	18
.3 GUV-3 Arbitrary Public Key Setting In Privileged Functions - Informational	19
.4 GUV-4 Missing Event Emission For Critical Access Control Operations - Informational	20

About Us

Guvenkaya is a security research firm specializing in Rust security, Web3 security of Non-EVM protocols, and Web2 security. With our expertise, we provide both security auditing services and custom security solutions

About Aurora

Aurora is a Virtual Chain built on NEAR. It's, at the same time, the sandbox and the proof of the robustness of the parent protocol. It's a smart contract - probably the most complex that exists - that is also an Ethereum Virtual Machine, providing a turn-key solution for developers to operate their apps on an Ethereum-compatible, high-throughput, scalable and future-safe platform, with low transaction costs.

Audit Results

Guvenkaya conducted a security assessment of the **NEAR Intents** from 12th February 2025 to 5th March 2025. NEAR Intents are a new type of transaction that allow information, requests, assets, and actions to be exchanged between AI agents, services, and end users. During this engagement, a total of **4 findings** were reported. 1 of the findings was medium and the remaining were either low or informational severity. The Aurora team has not fixed the issues yet.

Project Scope

Files	Link
Admin Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/admin-utils/src/lib.rs
Full Access Keys	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/admin-utils/src/full_access_keys.rs
Bitmap Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/bitmap/src/lib.rs
Borsh Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/borsh-utils/src/lib.rs
Base64	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/borsh-utils/src/base64.rs
String	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/borsh-utils/src/string.rs
Controller Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/controller/src/lib.rs
Core Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/lib.rs
Accounts	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/accounts.rs
Deadline	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/deadline.rs

Files	Link
Engine Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/engine/mod.rs
Engine Inspector	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/engine/inspector.rs
State Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/engine/state/mod.rs
State Cached	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/engine/state/cached.rs
State Deltas	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/engine/state/deltas.rs
Error	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/error.rs
Events	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/events.rs
Fees	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/fees.rs
Intents Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/intents/mod.rs
Intent Account	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/intents/account.rs
Token Diff	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/intents/token_diff.rs
Tokens (Intents)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/intents/tokens.rs
Nonce	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/nonce.rs
Payload Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/mod.rs

Files	Link
ERC191 Payload	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/erc191.rs
Multi Payload	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/multi.rs
NEP413 Payload	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/nep413.rs
Raw Payload	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/raw.rs
WebAuthn Payload	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/payload/webauthn.rs
Tokens (Core)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/core/src/tokens.rs
Crypto Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/lib.rs
Curve Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/curve/mod.rs
ED25519	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/curve/ed25519.rs
P256	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/curve/p256.rs
Secp256k1	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/curve/secp256k1.rs
Payload (Crypto)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/payload.rs
Public Key	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/public_key.rs
Serde Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/serde/mod.rs

Files	Link
Serde Curve	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/serde/curve.rs
Signature	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/crypto/src/signature.rs
Defuse Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/lib.rs
Accounts (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/accounts.rs
Contract Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/mod.rs
ABI	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/abi.rs
Accounts Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/accounts/mod.rs
Account	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/accounts/account.rs
State (Accounts)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/accounts/state.rs
Admin	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/admin.rs
Config	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/config.rs
Events (Contract)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/events.rs
Fees (Contract)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/fees.rs
Intents Mod (Contract)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/intents/mod.rs

Files	Link
Execute	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/intents/execute.rs
Relayer	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/intents/relayer.rs
Simulate	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/intents/simulate.rs
State (Intents)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/intents/state.rs
State (Contract)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/state.rs
Tokens Mod (Contract)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/mod.rs
NEP141 Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep141/mod.rs
NEP141 Deposit	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep141/deposit.rs
NEP141 Native	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep141/native.rs
NEP141 Withdraw	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep141/withdraw.rs
NEP171 Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep171/mod.rs
NEP171 Deposit	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep171/deposit.rs
NEP171 Withdraw	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep171/withdraw.rs
NEP245 Mod	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep245/mod.rs

Files	Link
NEP245 Core	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep245/core.rs
NEP245 Deposit	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep245/deposit.rs
NEP245 Resolver	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep245/resolver.rs
NEP245 Withdraw	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/tokens/nep245/withdraw.rs
Upgrade	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/contract/upgrade.rs
Fees (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/fees.rs
Intents (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/intents.rs
Tokens Mod (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/tokens/mod.rs
NEP141 (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/tokens/nep141.rs
NEP171 (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/tokens/nep171.rs
NEP245 (Defuse)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/defuse/src/tokens/nep245.rs
ERC191 Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/erc191/src/lib.rs
Map Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/lib.rs
BTree Map	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/btree_map.rs

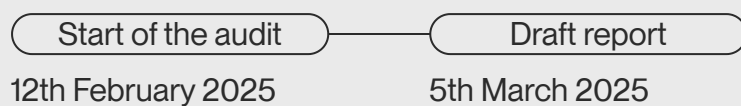
Files	Link
Cleanup	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/cleanup.rs
Hash Map	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/hash_map.rs
Iter	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/iter.rs
Near (Map Utils)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/map-utils/src/near.rs
Near Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/near-utils/src/lib.rs
Cache	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/near-utils/src/cache.rs
Gas	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/near-utils/src/gas.rs
Panic	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/near-utils/src/panic.rs
Prefix	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/near-utils/src/prefix.rs
NEP245 Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/lib.rs
Core (NEP245)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/core.rs
Events (NEP245)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/events.rs
Receiver	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/receiver.rs
Resolver (NEP245)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/resolver.rs

Files	Link
Token	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep245/src/token.rs
NEP413 Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep413/src/lib.rs
NEP461 Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/nep461/src/lib.rs
Num Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/num-utils/src/lib.rs
Serde Utils Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/serde-utils/src/lib.rs
Base58	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/serde-utils/src/base58.rs
Base64 (Serde)	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/serde-utils/src/base64.rs
WebAuthn Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/webauthn/src/lib.rs
WNEAR Lib	https://github.com/near/intents/blob/6da9e2b3ab598f277d45fb356aee01a5d80ac0a6/wnear/src/lib.rs

Out of Scope

The audit will include reviewing the code for security vulnerabilities. The audit does not include a review of the tests and dependencies.

Timeline



Methodology

RESEARCH INTO PROJECT ARCHITECTURE

PREPARING ATTACK VECTORS

SETTING UP AN ENVIRONMENT

MANUAL CODE REVIEW OF THE CODE

ASSESSMENT OF RUST SECURITY ISSUES

ASSESSMENT OF NEAR SECURITY ISSUES

ASSESSMENT OF ARITHMETIC ISSUES

BUSINESS LOGIC VULNERABILITY ASSESSMENT

ONCHAIN TESTING USING NEAR WORKSPACES

BEST PRACTICES AND CODE QUALITY

CHECKING FOR CODE REFACTORING/SIMPLIFICATION POSSIBILITIES

ARCHITECTURE IMPROVEMENT SUGGESTIONS

PREPARING POCS AND/OR TESTS FOR EACH CRITICAL/HIGH/MEDIUM ISSUES

Severity Breakdown

01. Likelihood Ratings

Likely: The vulnerability is easily discoverable and not overly complex to exploit.

Possible: The vulnerability presents some challenges either in discovery or in the complexity of the attack.

Rare: The vulnerability is either very difficult to discover or complex to exploit, or both.

This matrix provides a nuanced view, taking into account both the ease of discovering a vulnerability and the complexity involved in exploiting it.

02. Impact

Severe: The vulnerability is easily discoverable and not overly complex to exploit.

Moderate: The vulnerability presents some challenges either in discovery or in the complexity of the attack.

Negligible: The vulnerability is either very difficult to discover or complex to exploit, or both.

03. Severity Ratings

Critical: Assigned to vulnerabilities with severe impact and a likely likelihood of exploitation.

High: For vulnerabilities with either severe impact but only a possible likelihood, or moderate impact with a likely likelihood.

Medium: Used for vulnerabilities with severe impact but a rare likelihood, moderate impact with a possible likelihood, or negligible impact with a likely likelihood.

Low: For vulnerabilities with moderate impact and rare likelihood, or negligible impact with a possible likelihood.

Informational: The lowest severity rating, typically for vulnerabilities with negligible impact and a rare likelihood of exploitation.

CRITICAL**HIGH****MEDIUM**

Low

Informational

Likelihood Matrix:

Attack Complexity \ Discovery Ease	Obvious	Concealed	Hidden
Complex	Possible	Rare	Rare
Moderate	Likely	Possible	Rare
Straightforward	Likely	Possible	Possible

Likelihood/Impact Matrix:

Likelihood \ Impact	Severe	Moderate	Negligible
Likely	CRITICAL	HIGH	MEDIUM
Possible	HIGH	MEDIUM	Low
Rare	MEDIUM	Low	Informational

Findings Summary

01. Remediation Complexity: This measures how difficult it is to fix the vulnerability once it has been identified.

Simple: Patches or fixes are readily available and easily implemented.

Moderate: Requires some time and resources to remediate, but well within the capabilities of most organizations.

Difficult: Remediation requires significant resources, specialized skills, or substantial changes to systems or architecture.

02. Status: This measures how difficult it is to fix the vulnerability once it has been identified.

Not Fixed: Indicates that the vulnerability has been identified but no remedial action has been taken yet. This status is crucial for newly discovered vulnerabilities or those awaiting prioritization.

Fixed: This status is applied when the vulnerability has been successfully remediated. It implies that appropriate measures (like patching, configuration changes, or architectural modifications) have been implemented to resolve the issue.

Acknowledged: This status is used for vulnerabilities that have been recognized, but for various reasons (such as risk acceptance, cost, or other business decisions), have not been fixed. It indicates that the risk posed by the vulnerability is known and has been consciously accepted.

Scheduled: This status indicates that the vulnerability has been acknowledged and a plan is in place to fix it in the future. It signifies that while remediation hasn't yet occurred, the issue has been prioritized and is part of the planned development roadmap.

Finding	Impact	Likelihood	Severity	Remediation Complexity	Remediation Status
GUV-1: Potential Funds Stealing From Users Via Repeating Failed Intents	Severe	Rare	MEDIUM	Simple	Scheduled
GUV-2: Possible DoS Of Public Keys Viewing Per User	Negligible	Possible	Low	Simple	Not Fixed
GUV-3: Arbitrary Public Key Setting In Privileged Functions	Negligible	Rare	Informational	Simple	Not Fixed
GUV-4: Missing Event Emitting In Privileged Functions	Negligible	Rare	Informational	Simple	Not Fixed

Findings Details

GUV-1 Potential Funds Stealing From Users Via Repeating Failed Intents - Medium

Depending on the intent structure, it's possible to maliciously fail a transaction and then repeat specific intents, which could lead to:

- Stealing tokens
- Making solvers lose money or perform unauthorized operations

Mainnet deadlines are permissive, ranging from 20 seconds to 10 minutes. This provides ample time to fail a transaction and repeat failed intents. A transaction can be failed by:

- Invalidating the nonce after signing in a separate transaction.
- Adding an additional intent to your intent array that transfers funds out and fails your token diff

Malicious actor can:

- Repeat selected intents.
- Repeat selected intents and, to maintain **TokenDiff** balance, resign your controlled intents with new values.
- Observe failed intents on the blockchain and reconstruct them like building blocks (while deadlines remain valid).

The risk is low when **TokenDiff** intent is used, as mainnet calculations are typically precise, making it difficult to modify the intent structure while maintaining zero delta and gaining benefits. The vulnerability is particularly dangerous in **P2P** transfer scenarios where **TokenDiff** intent isn't used, allowing for immediate exploitation with high success rates.

Impact:

Funds can be stolen in scenarios where **TokenDiff** intent isn't used.

Recommendation

This behavior should be documented to emphasize that TokenDiff is the preferred method, while Transfer should be discouraged for facilitating swaps. Users must understand they are responsible for reviewing and approving what they sign.

Remediation - Scheduled

The Aurora team has acknowledged the issue and will fix it soon by documenting this scenario.

GUV-2 Possible DoS Of Public Keys Viewing Per User - Low

It was observed that since user can have unlimited public keys, it is possible for a malicious user to cause a DoS of **public_keys_of** method when their account is used. That's because **public_keys_of** iterates over public keys of a provided account and if account has a lot of public keys it can lead to the error due to a gas limit.

defuse/src/contract/accounts/mod.rs

```
fn public_keys_of(&self, account_id: &AccountId) -> HashSet<PublicKey> {
    self.accounts.get(account_id).map_or_else(
        || {
            PublicKey::from_implicit_account_id(account_id)
                .into_iter()
                .collect()
        },
        |account| account.iter_public_keys(account_id).collect(),
    )
}
```

Impact:

- Errors in off-chain components, which utilize **public_keys_of** method.
- If **iter_public_keys** is utilized within the smart contract logic somewhere else, depending on a logic it can lead to the DoS on protocol level

Recommendation

It is recommended to limit the number of public keys each account can have

Remediation - Not Fixed

The Aurora team has not fixed the issue yet.

GUV-3 Arbitrary Public Key Setting In Privileged Functions - Informational

The codebase accepts public keys in multiple locations without proper validation. The NEAR SDK's **PublicKey** type lacks comprehensive validation of public key formats and values. Malicious users could potentially inject invalid or malformed public keys, leading to undefined behavior in cryptographic operations.

PoC:

рос

```
fn test_parse_zero_pubkey() {
    use near_sdk::PublicKey;
    let zero_pubkey_str = "ed25519:11111111111111111111111111111111";
    let result = zero_pubkey_str.parse::<PublicKey>();
    assert!(result.is_err());
}
```

Impact:

- Potential undefined behavior in cryptographic operations
- Potential injection of weak public keys that can lead to signature malleability

Recommendation

Implement comprehensive validation for public keys in all relevant functions.

- Account Public Key Management (add_public_key, remove_public_key)
- Relay Keys Management (do_add_relayer_key, delete_relayer_key)
- Full Access Keys Management (add_full_access_key, delete_key)

Remediation - Not Fixed

The Aurora team has not fixed the issue yet.

GUV-4 Missing Event Emission For Critical Access Control Operations - Informational

The relay key operations lacks event emissions for access control operations in **delete_relayer_key()** and **do_add_relayer_key()** methods. This omission makes it difficult to track and audit changes to the relay key set off-chain. Events are essential for maintaining transparency and allowing external systems to monitor and react to important state changes in the contract.

Recommendation

Implement event emissions for both adding and removing relay key

Remediation - Not Fixed

The Aurora team has not fixed the issue yet.