Scout Report - 2025-09-27

Summary

Crate	Status	Critical	Medium	Minor	Enhancement
authority	Analyzed	5	4	1	2
protocol	Analyzed	2	0	0	3
resolvers	Analyzed	0	0	0	0

Issues found:

- Front Running (2 results) (Medium)
- Integer Overflow Or Underflow (7 results) (Critical)
- Unused Return Enum (1 results) (Minor)
- Unnecessary Admin Parameter (2 results) (Medium)
- Soroban Version (5 results) (Enhancement)

MEV

Front Running

Impact: Medium

Description: The transferred amount should be checked against a minimum to prevent front-running

More about: here

ID	Package	Detection
6	authority	resolver.rs:111:5 - 111:77
7	authority	resolver.rs:152:5 - 152:77

Arithmetic

Integer Overflow Or Underflow

Impact: Critical

Description: Potential for integer arithmetic overflow/underflow. Consider checked, wrapping or saturating arithmetic.

More about: here

ID	Package	Detection
1	protocol	attestation.rs:173:21 - 173:30
2	protocol	delegation.rs:223:21 - 223:38
8	authority	state.rs:86:27 - 86:56
9	authority	state.rs:116:27 - 116:56
10	authority	state.rs:148:22 - 148:49
11	authority	state.rs:167:22 - 167:49
12	authority	lib.rs:48:25 - 48:54

Error Handling

Unused Return Enum

Impact: Minor

Description: If any of the variants (Ok/Err) is not used, the code could be simplified or it could imply a bug

More about: here

ID	Package	Detection
13	authority	lib.rs:269:9 - 269:15

Authorization

Unnecessary Admin Parameter

Impact: Medium

Description: Usage of admin parameter might be unnecessary

More about: here

ID	Package	Detection
15	authority	lib.rs:219:42 - 219:56
16	authority	lib.rs:57:9 - 57:23

Best Practices

Soroban Version

Impact: Enhancement

Description: Use the latest version of Soroban

More about: here

Storage Change Events

Impact: Enhancement

Description: Consider emiting an event when storage is modified

More about: here

ID	Package	Detection
0	protocol	lib.rs:1:1 - 1:1
3	protocol	lib.rs:137:5 - 137:104
4	protocol	lib.rs:36:5 - 36:77
5	authority	lib.rs:1:1 - 1:1

ID	Package	Detection
14	authority	lib.rs:32:5 - 37:27