Uncaught Panic in ORML Rewards Pallet

High xlc published GHSA-5v93-9mqw-p9mh on Feb 14, 2025

Package	Affected versions	Patched versions
orml-rewards (Rust)	<1.1.0	1.2.1

Severity

High

CVE ID

No known CVE

Weaknesses

No CWEs

Description

Summary

A vulnerability in the `add_share` function of the **Rewards** pallet (part of the ORML repository) can lead to an uncaught Rust panic when handling user-provided input exceeding the `u128` range.

Affected Components

- **ORML Rewards** pallet (`rewards/src/lib.rs`)
- Any Substrate-based chain using ORML Rewards with `add_share` accepting unvalidated large `u128` inputs

Technical Details

- `add_share` performs arithmetic on user-supplied values (`add_amount`) of type `T::Share` (mapped to `u128` in Acala).
- If `add_amount` is large enough (e.g., `i128::MAX`), the intermediate result may overflow and panic on the cast to `u128` .
- Validation occurs only after arithmetic, enabling a crafted input to trigger an overflow.

Impact

A malicious user submitting a specially crafted extrinsic can cause a panic in the runtime:

- **Denial of Service** by crashing the node process.
- **Potential for invalid blocks** produced by validators.

Likelihood

This issue is exploitable in production if there exists at least one rewards pool where reward tokens exceed twice the collateral tokens, allowing sufficiently large multiplication to exceed `u128` bounds.

Remediation

- This issue is fixed in #1016

Backport

The patch have been backported to following release branches:

- polkadot-stable2407
- polkadot-stable2409

A 1.0.1 patch release is made with this fix.