Gossipsub PRUNE Backoff Heartbeat Instant Overflow

High **jxs** published **GHSA-xqmp-fxgv-xvq5** 4 days ago

Package

libp2p-gossipsub (Rust)

Affected versions	Patched versions
< v0.49.4	v0.49.4

Description

Description

Summary

The Rust libp2p Gossipsub implementation contains a remotely reachable panic in `backoff` expiry handling.
After a peer sends a crafted `PRUNE` control message with an attacker-controlled, near-maximum `backoff` value, the value is accepted and stored as an `Instant` near the representable upper bound.
On a later heartbeat, the implementation performs unchecked `Instant + Duration` arithmetic (`backoff_time + slack`), which can overflow and panic with:
`overflow when adding duration to instant`
This issue is reachable from any Gossipsub peer over normal `TCP + Noise + mplex/yamux` connectivity and requires no further authentication beyond becoming a protocol peer.

Attack Scenario

An attacker that can establish a libp2p Gossipsub session with a target node can crash the target by sending crafted `PRUNE` control data:

1. Establish a standard libp2p session (`TCP + Noise`) and negotiate a stream multiplexer (`mplex` / `yamux`).
2. Open a Gossipsub stream and send an RPC containing `ControlPrune` with a very large `backoff` (chosen near boundary conditions, e.g. `~ i64::MAX - victim_uptime_seconds`; example

observed: `9223372036854674580` for ~28h uptime).

3. The value is parsed from protobuf and passed through `Behaviour::handle_prune()` into mesh/backoff update logic.
4. Initial storage path uses checked addition (`Instant::now().checked_add(...)`), so the malicious near-max value is retained.
5. On the next heartbeat (typically within ~43–74s), expiry logic computes `backoff_time + slack` using unchecked addition, which overflows and panics.

Impact

Remote unauthenticated denial of service (critical).
Any application exposing an affected `libp2p-gossipsub` listener can be crashed by a network-reachable peer that sends crafted `PRUNE` backoff values. The crash is triggered during heartbeat processing (not immediately at PRUNE parse time), and can be repeated by reconnecting and replaying the message.

Differences from CVE-2026-33040

This advisory is related to CVE-2026-33040 but it is not the same defect. CVE-2026-33040 addressed overflow during backoff insertion by adding checked arithmetic when converting PRUNE backoff into an Instant. The issue in this advisory occurs at a different location and at a different time: a near-maximum backoff can still be stored successfully, and the crash happens later in the heartbeat path when slack is added to that stored Instant using unchecked arithmetic. This report covers a distinct secondary overflow path in heartbeat expiry handling that remained reachable after the original insertion-side hardening.

This vulnerability was originally reported by the Security team of the Ethereum Foundation.

Severity

High 8.2 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	None

Availability	High

Subsequent System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-34219

Weaknesses

No CWEs