Unbounded rendezvous DISCOVER cookies enable remote memory exhaustion

High **jxs** published **GHSA-v5hw-cv9c-rpg7** 5 days ago

Package

libp2p-rendezvous (Rust)

Affected versions	Patched versions
< 0.17.1	0.17.1

Description

Summary

The rendezvous server stores pagination cookies without bounds.
An unauthenticated peer can repeatedly issue `DISCOVER` requests and force unbounded memory growth.

Details

Pagination state is stored in:

```
HashMap<Cookie, HashSet<RegistrationId>>
```

On `Message::Discover`:

```
remote peer
→ DISCOVER
→ handle_request
→ registrations.get(...)
→ new cookie generated
→ cookie inserted into Registrations::cookies
```

There is **no upper bound or eviction policy**, so repeated DISCOVER requests grow this map indefinitely.

PoC

A reproduction test and minimal harness will be provided in a private fork in a follow-up comment.

Impact

Remote state amplification leading to memory exhaustion.

Properties:

- etwork reachable
- no authentication required
- low attack complexity
- protocol-compliant traffic

Impacts rendezvous nodes exposed to untrusted peers.

Possible Fixes

1. **Global cap + eviction**

Bound cookie storage (`MAX_COOKIES_TRACKED`) with FIFO/expiry aware eviction.
Tradeoff: attacker can churn cookies and evict legitimate pagination state.

2. **Stateless cookies**

Encode pagination state in authenticated cookies instead of storing server-side state.
Tradeoff: more complex implementation.

3. **Rate limiting / per-peer quotas**

Limit cookie creation per peer.
Tradeoff: requires peer tracking.

Severity

High 8.2 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low

Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

CVE ID

CVE-2026-35457

Weaknesses

No CWEs

Credits

failuresmith Reporter