rack / **rack-session** Public

Code | Issues 4 | Pull requests | Discussions | Actions | Projects | **Security** 1

`Rack::Session::Pool` sessions can be restored after deletion

Moderate **ioquatix** published **GHSA-9j94-67jr-4cqj** 3 days ago

Package	Affected versions	Patched versions
rack-session (RubyGems)	>= 2.0.0, < 2.1.1	2.1.1

Description

Summary

When using the `Rack::Session::Pool` middleware, simultaneous rack requests can restore a deleted rack session, which allows the unauthenticated user to occupy that session.

Details

Rack session middleware prepares the session at the beginning of request, then saves is back to the store with possible changes applied by host rack application. This way the session becomes to be a subject of race conditions in general sense over concurrent rack requests.

Impact

When using the `Rack::Session::Pool` middleware, and provided the attacker can acquire a session cookie (already a major issue), the session may be restored if the attacker can trigger a long running request (within that same session) adjacent to the user logging out, in order to retain illicit access even after a user has attempted to logout.

Mitigation

- Update to the latest version of `rack-session`, or
- Ensure your application invalidates sessions atomically by marking them as logged out e.g., using a `logged_out` flag, instead of deleting them, and check this flag on every request to prevent reuse, or
- Implement a custom session store that tracks session invalidation timestamps and refuses to accept session data if the session was invalidated

Severity

Moderate 4.2 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2025-46336

Weaknesses

CWE-362 CWE-367 CWE-613

Credits

stengineering0	Reporter
jeremyevans	Remediation develo
ioquatix	Coordinator

after the request began.

Related

This code was previously part of `rack` in Rack < 3, see GHSA-vpfw-47h7-xj4g for the equivalent advisory in `rack` (affecting Rack < 3 only).