Login timing side-channel reveals user existence

Moderate **mtrezza** published **GHSA-mmpq-5hcv-hf2v** 2 days ago

Package

parse-server (npm)

Affected versions	Patched versions
>= 9.0.0, < 9.8.0-alpha.6	9.8.0-alpha.6
< 8.6.74	8.6.74

Description

Impact

The login endpoint response time differs measurably depending on whether the submitted username or email exists in the database. When a user is not found, the server responds immediately. When a user exists but the password is wrong, a bcrypt comparison runs first, adding significant latency. This timing difference allows an unauthenticated attacker to enumerate valid usernames.

Patches

A dummy bcrypt comparison is now performed when no user is found, normalizing response timing regardless of user existence. Additionally, accounts without a stored password (e.g. OAuth-only) now also run a dummy comparison to prevent the same timing oracle.

Workarounds

Configure rate limiting on the login endpoint to slow automated enumeration. This reduces throughput but does not eliminate the timing signal for individual requests.

References

- GitHub security advisory: GHSA-mmpq-5hcv-hf2v
- Fix Parse Server 9: #10398

- Fix Parse Server 8: #10399

Severity

Moderate 6.3 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	High
Attack Requirements	Present
Privileges Required	None
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	Low
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-39321

Weaknesses

▶ CWE-208

Credits

offset	Reporter
mtrezza	Coordinator