

parse-community / parse-server Public[Code](#) [Issues](#) 370 [Pull requests](#) 102 [Actions](#) [Projects](#) [Wiki](#) [Security](#)

# Auth data exposed via verify password endpoint

High mtrezza published **GHSA-wp76-gg32-8258** last week

## Package

 **parse-server** ([npm](#))

### Affected versions

$\geq 9.0.0, < 9.7.0\text{-alpha.7}$   
 $< 8.6.63$

### Patched versions

$9.7.0\text{-alpha.7}$   
 $8.6.63$

## Description

### Impact

The verify password endpoint returns unsanitized authentication data, including MFA TOTP secrets, recovery codes, and OAuth access tokens. An attacker who knows a user's password can extract the MFA secret to generate valid MFA codes, defeating multi-factor authentication protection.

### Patches

The verify password endpoint now sanitizes authentication data through auth adapter hooks before returning the response, consistent with login and user retrieval endpoints.

### Workarounds

There is no known workaround.

### References

- GitHub security advisory: [GHSA-wp76-gg32-8258](#)
- Fix Parse Server 9: [#10323](#)
- Fix Parse Server 8: [#10324](#)

Severity

High 8.2 / 10

CVSS v4 base metrics

Exploitability Metrics

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

Vulnerable System Impact Metrics

Confidentiality	High
Integrity	None
Availability	None

Subsequent System Impact Metrics

Confidentiality	High
Integrity	None
Availability	None

[Learn more about base metrics](#)

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

CVE ID

CVE-2026-34215

Weaknesses

► CWE-200

Credits

 offset

Reporter

 mtrezza

Coordinator