OAuth account takeover via auto-linking

Critical **BijjuXD** published **GHSA-8mcf-rp68-xhfg** last week

Package

php **reviactyl/panel** (Composer)

Affected versions	Patched versions
>= 26.2.0-beta.1	26.2.0-beta.5

Description

Impact

A vulnerability in the OAuth authentication flow allowed automatic linking of social accounts based solely on matching email addresses.

An attacker could create or control a social account (e.g., Google, GitHub, Discord) using a victim's email address and gain full access to the victim's account without knowing their password.

This results in a **full account takeover** with no prior authentication required.

Patches

This issue has been patched in **v26.2.0-beta.5**

Users running **v26.x.x releases** should upgrade immediately to the latest version to mitigate the vulnerability.

Workarounds

Users must upgrade to a patched version. As a temporary mitigation, disabling all OAuth login providers can reduce exposure until the update is applied.

References

- Fix commit: `fe0c29f`
- Fixed Release: https://github.com/reviactyl/panel/releases/tag/v26.2.0-beta.5

identified and fixed by Aymen Elouadi

Severity

Critical 9.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34456

Weaknesses

▶ CWE-284

Credits

aymenelouadi Finder