Any password authenticates banned accounts and grants API access

Critical **seanscodes** published **GHSA-9vx4-7ww7-4cf5** 2 days ago

Package

Polarlearn

Affected versions

<= v0-PRERELEASE-15

Patched versions

None

Description

Summary

`POST /api/v1/auth/sign-in` creates a valid session for banned accounts before verifying the supplied password. That session is then accepted across authenticated `/api` routes, enabling account data access and authenticated actions as the banned user.

Details

`signInCredentials()` loads the user record, computes a hash for the attacker-supplied password, and then returns early when `loginAllowed === false`. In that branch it calls `createSession(user.id)` and returns a banned response without ever comparing the supplied password to the stored password hash.

The public sign-in endpoint exposes this behavior directly and returns success for banned users. The intended ban enforcement only exists in `proxy.ts`, but that middleware explicitly skips all `/api` paths. `getUserFromSession()` also does not reject banned users, so the issued session is accepted by authenticated API routes. For example, `GET /api/v1/settings/export` returns the signed-in user's exported account data, and other authenticated mutation endpoints remain reachable as well.

Exploit conditions:

- the target account must already be banned
- the attacker must know the target email address
- if Turnstile is enabled, a valid `captchaToken` is also required

Impact

Anyone who knows a banned user’s email address can log in as that user with an arbitrary password, read that account’s exported data, and perform authenticated API actions as the victim until the session expires.

Severity

Critical 9.2 / 10

CVSS v4 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-39322

Weaknesses

▶ CWE-287

Credits

 **Jvr2022** Reporter

 **seanscodes** Coordinator