better-auth: OAuth Proxy lets an attacker sign in as another user

High severity | GitHub Reviewed | Published on Sep 30 in **better-auth/better-auth** • Updated 3 weeks ago

Vulnerability details | Dependabot alerts 0

Package	Affected versions	Patched versions
better-auth (npm)	>= 1.5.0-beta.12, < 1.7.7	1.7.7

Description

Am I affected?

You may be affected if you use `better-auth` from 1.5.0-beta.12 through versions before 1.7.7 with the OAuth Proxy plugin. You are affected only if **all** of these are also true:

- On a participating environment, the OAuth Proxy plugin has no dedicated `secret`, or its `secret` equals that environment's global Better Auth secret.
- Sign-in state is stored in a cookie (`account.storeStateStrategy: "cookie"`). With a database or secondary storage, this is only the case if you chose it explicitly.
- Implicit account linking is on (the default).

You are not affected by this path if every participating environment uses a proxy `secret` distinct from its global Better Auth secret, if sign-in state is stored in the database, or if you use a version before 1.5.0-beta.12.

Summary

The OAuth Proxy plugin trusts any user profile it can decrypt. In the affected setup, Better Auth encrypts sign-in state, including data the caller chose, with the same secret and hands it to anyone who starts a social sign-in. An attacker can use this to get a fake profile for another user's email address that the proxy accepts as real.

Impact

An attacker without an account who knows a user's verified email address can sign in as that user, with that user's permissions. They can read private data, change the account, and link a provider account of their choice to it. They need no provider sign-in and no action from the victim. No availability impact is established, and a reported open redirect was not confirmed.

Patches

The fix is merged for the planned `better-auth` 1.7.7 release. That package is not available yet.

Upgrade all nodes handling the same cookie-backed OAuth or SAML state flow and all OAuth Proxy participants together, including the production coordinator and preview or development deployments. Keep installed Better Auth packages released alongside `better-auth` on the same release version. Restart pending sign-in and account-linking flows; pre-upgrade state cookies and proxy payloads are rejected. Public options and API signatures are unchanged.

Workarounds

Until you upgrade to the fixed release, apply one of these:

- Set one strong OAuth Proxy `secret` across every environment that takes part in the proxy flow, and keep it different from each environment's global Better Auth secret.
- Set `account.storeStateStrategy: "database"`. This is already the default when a database or secondary storage is configured. If Magic Link is also enabled, switching can expose a separate cross-purpose verification-record path in affected releases. Ensure the two flows resolve to distinct stored identifiers; with built-in options, use Magic Link `storeToken: "hashed"` with global `verification.storeIdentifier` unset or `"plain"`, or disable Magic Link or both built-in social and Generic OAuth sign-in.
- Remove the OAuth Proxy plugin if you do not need it.

Setting `account.accountLinking.disableImplicitLinking: true` stops this path from taking over an existing account. It does not fix the underlying flaw: the callback can still accept attacker-made data as a provider identity. Apply one of the steps above as well.

Severity

High 7.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
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:H/PR:N/UI:N/S:U/C:H/I:H/A:N

EPSS score

Weaknesses

- CWE-287
- CWE-345

CVE ID

No known CVE

GHSA ID

GHSA-r4xp-prcw-77qf

Source code

better-auth/better-auth

Credits

iabdullah215 Reporter

martinfrancois Reporter

See something to contribute? Suggest improvements for this vulnerability.

References

- GHSA-r4xp-prcw-77qf
- better-auth/better-auth#11494
- better-auth/better-auth@ `ac54bfd`
- https://github.com/better-auth/better-auth/releases/tag/v1.7.7



gustavovalverde published to better-auth/better-auth on Sep 30

Published to the GitHub Advisory Database 3 weeks ago

Reviewed 3 weeks ago

Last updated 3 weeks ago

Terms Privacy Security Status Community Docs Contact Manage cookies
Do not share my personal information

© 2026 GitHub, Inc.