Account takeover via SSO plugins (via shared link to /auth/callback with valid code)

High **julianlam** published **GHSA-xmgg-fx9p-prq6** on Sep 1

Package

nodebb (npm)

Affected versions	Patched versions
< 1.17.1	1.17.2

Description

This is a historical security advisory, pertaining to a vulnerability that was reported, patched, and published in 2021. It is listed here for completeness and for CVE tracking purposes.

Impact

Due to an unnecessarily strict conditional in the code handling the first step of the SSO process, the pre-existing logic that added (and later checked) a nonce was inadvertently rendered opt-in instead of opt-out.

This re-exposed a vulnerability in that a specially crafted MITM attack could theoretically take over another user account during the single sign-on process.

Patches

The issue has been fully patched as of v1.17.2.

The patch commit can be found at `a2400f6`

Workarounds

Site maintainers can cherry-pick `a2400f6` into their codebase to patch the exploit.

References

- https://blogs.opera.com/security/2022/03/bug-bounty-adventures-a-nodebb-0-day/

For more information

If you have any questions or comments about this advisory:

- Discuss it on our community forum
- Email us at support@nodebb.org

Severity

High

CVE ID

CVE-2022-36076

Weaknesses

CWE-352