JWT Signature Verification Bypass Allows Authentication as Arbitrary Users

Critical **ericwang401** published **GHSA-92pg-3w49-4w5x** 5 days ago

Package

convoypanel/panel

Affected versions

>= v3.9.0-beta, < 4.5.1

Patched versions

>= 4.5.1

Description

Impact

The `JWTService::decode()` method did not verify the cryptographic signature of JWT tokens. While the method configured a symmetric HMAC-SHA256 signer via `lcobucci/jwt`, it only validated time-based claims (`exp`, `nbf`, `iat`) using the `StrictValidAt` constraint. The `SignedWith` constraint was not included in the validation step.

This means an attacker could forge or tamper with JWT token payloads — such as modifying the `user_uuid` claim — and the token would be accepted as valid, as long as the time-based claims were satisfied. This directly impacts the SSO authentication flow (`LoginController::authorizeToken`), allowing an attacker to authenticate as any user by crafting a token with an arbitrary `user_uuid`.

All Convoy installations prior to v4.5.1 that use JWT-based SSO authentication are affected.

Patches

This vulnerability is patched in **v4.5.1**. The `SignedWith` constraint has been added to the JWT validation logic in `JWTService::decode()`, ensuring that tokens with invalid or missing signatures are rejected.

Users should upgrade to v4.5.1 or later immediately.

Workarounds

There are no workarounds. The signature verification was entirely absent from the decode path, so the only remediation is to upgrade to the patched version. Disabling the SSO login endpoint would mitigate exposure but is not practical for most deployments.

References

- lcobucci/jwt documentation on validation constraints
- CWE-347: Improper Verification of Cryptographic Signature

Severity

Critical 9.8 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33746

Weaknesses

- CWE-287
- CWE-347

Credits

justlife4x4 Reporter