Vaultwarden: WebAuthn assertion processed before signature verification allows persistent credential backup-flag tampering

Moderate **dani-garcia** published **GHSA-x7g7-cgx5-jhx2** last week

Package

vaultwarden (Rust)

Affected versions	Patched versions
<= 1.35.4	1.35.5

Description

Summary

Vaultwarden updates persistent WebAuthn credential metadata based on unverified authenticatorData before signature validation during the WebAuthn authentication flow.

An attacker who knows a user's password but cannot produce a valid WebAuthn signature can still permanently modify the stored backup_eligible and backup_state flags for that user's credential.

This can result in permanent denial of service of WebAuthn 2FA for affected credentials.

Details

In `validate_webauthn_login()`

```
check_and_update_backup_eligible(...);
let authentication_result =
    WEBAUTHN.finish_passkey_authentication(...)?;
```

`check_and_update_backup_eligible()` parses `rsp.response.authenticator_data and` updates the stored WebAuthn registration before calling `finish_passkey_authentication()`

The function extracts the Backup Eligible (BE) and Backup State (BS) flags directly from the unverified authenticatorData and persists them to the database.

However, `finish_passkey_authentication()` performs signature validation only afterward.

If signature verification fails, the database update is not rolled back.

PoC

1. Use a normal user account with an existing WebAuthn credential already registered.
2. Start a login that reaches the WebAuthn 2FA assertion step (so a login challenge state exists).
3. Submit a WebAuthn assertion response where:

- . `rawId` matches one of the user's registered credentials, and
- `response.authenticatorData[32]` (flags) is tampered to set BE=1 (and optionally toggle BS), but the signature is invalid (expected after tampering).

4. Observe: authentication fails, but the server updates the stored credential metadata (`backup_eligible` / `backup_state`) before signature verification and persists it.

Impact

An authenticated user can cause a persistent DB update of their WebAuthn credential's `backup_eligible` / `backup_state` metadata based on an unverified assertion response (i.e., even when signature verification fails), because the DB write occurs prior to `finish_passkey_authentication()`.

Severity

Moderate 4.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-31835

Weaknesses

▶ CWE-345

Credits

dorakemon	Reporter
BlackDex	Remediation verifier