vercel / **flags** Public

Code | Issues 8 | Pull requests 9 | Actions | **Security** 1 | Insights

Information Disclosure may allow all flags to be listed

Moderate **dferber90** published **GHSA-892p-pqrr-hxqr** yesterday

Package	Affected versions	Patched versions
@vercel/flags (npm)	<=3.1.1	flags 4.0.0
flags (npm)	<=3.2.0	4.0.0

Description

Summary

An information disclosure vulnerability affecting Flags SDK has been addressed. It impacted `flags` ≤3.2.0 and `@vercel/flags` ≤3.1.1 and in certain circumstances, allowed a bad actor with detailed knowledge of the vulnerability to list all flags returned by the flags discovery endpoint (`.well-known/vercel/flags`).

Impact

This vulnerability allowed for information disclosure, where a bad actor could gain access to a list of all feature flags exposed through the flags discovery endpoint, including the:

- Flag names
- Flag descriptions
- Available options and their labels (e.g. `true` , `false`)
- Default flag values

Not impacted:

- Flags providers were not accessible

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2025-46332

Weaknesses

CWE-200

No write access nor additional customer data was exposed, this is limited to just the values noted above. Vercel has automatically mitigated this incident on behalf of our customers for the default flags discovery endpoint at `.well-known/vercel/flags`. Flags Explorer will be disabled and show a warning notice until upgraded to `flags@4.0.0`.

Resolution

The `verifyAccess` function was patched within `flags@4.0.0`.

Users of `@vercel/flags` should also migrate to `flags@4.0.0`.

For further guidance on upgrading your version, please see our upgrade guide.

Mitigations

Vercel implemented a network-level mitigation to prevent the default flags discovery endpoint at `/.well-known/vercel/flags` being reachable, which automatically protects Vercel deployments against exploitation of this issue. Users need to upgrade to `flags@4.0.0` to re-enable the Flags Explorer.

This automatic mitigation is not effective in two scenarios:

- When using the Flags SDK on Pages Router, as the original non-rewritten route would still be accessible, e.g. `/api/vercel/flags`.
- When using a custom path for the flags discovery endpoint.

If you are not protected by the Vercel default mitigation you can temporarily deny access to the other exposed flags discovery endpoints through a custom WAF rule while you upgrade to the latest version.

References

- https://vercel.com/changelog/information-disclosure-in-flags-sdk-cve-2025-46332
- https://github.com/vercel/flags/blob/main/packages/flags/guides/upgrade-to-v4.md