

 [auth0 / nextjs-auth0](#) Public[Code](#) [Issues 8](#) [Pull requests 20](#) [Discussions](#) [Actions](#) [Security and](#)

Improper Proxy Cache Lookup in the Auth0 Next.js SDK

Moderate [jennyang-okta](#) published [GHSA-xq8m-7c5p-c2r6](#) 8 hours ago

Package

 [@auth0/nextjs-auth0](#) ([npm](#))

Affected versions

$\geq 4.12.0$ and $\leq 4.17.0$

Patched versions

4.18.0

Description

Description

In affected versions of the Next.js SDK, simultaneous requests that trigger a nonce retry may cause the proxy cache fetcher to perform improper lookups for the token request results.

Am I Affected?

You are affected if you meet all of the following preconditions:

- Applications using the auth0/nextjs-auth0 SDK, versions 4.12.0 to 4.17.0, and
- Applications using the proxy handler `/me/*` and `/my-org/*` with DPoP enabled.

Affected product and versions

Auth0/nextjs-auth0 v4.12.0 to 4.17.0

Resolution

Upgrade Auth0/nextjs-auth0 version to v4.18.0 or greater

Acknowledgements

Okta would like to thank Reynaldo Immanuel for their discovery and responsible disclosure.

Severity

Moderate 5.4 / 10

CVSS v3 base metrics

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

[Learn more about base metrics](#)

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

CVE ID

CVE-2026-40155

Weaknesses

- ▶ CWE-863