snyk

Snyk test report

January 7th 2025, 1:15:30 pm (UTC+00:00)

Scanned the following path:

- C:\Users\Dell\Documents\ECOLE IT\SOP\nextly-template-main/yarn.lock (yarn)

5 known vulnerabilities | 5 vulnerable dependency paths | 49 dependencies

Project	nextly-template	Path	C:\Users\Dell\Documents\ECOLE IT\SOP\nextly-template-main
Package Manager	yarn	Manifest	yarn.lock

HIGH SEVERITY

Acceptance of Extraneous Untrusted Data With Trusted Data

- Package Manager: npm
- Vulnerable module: next
- Introduced through: nextly-template@2.0.0 and next@14.2.3

Detailed paths

- *Introduced through*: nextly-template@2.0.0 › next@14.2.3

Overview

next is a react framework.

Affected versions of this package are vulnerable to Acceptance of Extraneous Untrusted Data With Trusted Data by sending a crafted HTTP request, which allows the attacker to poison the cache of a non-dynamic server-side rendered route in the page router. This will coerce the request to cache a route that is meant to not be cached and send a `Cache-Control: s-maxage=1, a stale-while-revalidate` header, which some upstream CDNs may cache as well.

Note:

This is only vulnerable if:

1. The user is using pages router
2. The user is using non-dynamic server-side rendered routes.

Users are not affected if:

1. They are using the app router
2. The deployments are on Vercel

Remediation

Upgrade `next` to version 13.5.7, 14.2.10 or higher.

References

- GitHub Commit
- GitHub Commit

More about this vulnerability

HIGH SEVERITY

Uncontrolled Recursion

- Package Manager: npm
- Vulnerable module: next
- Introduced through: nextly-template@2.0.0 and next@14.2.3

Detailed paths

- *Introduced through*: nextly-template@2.0.0 › next@14.2.3

Overview

next is a react framework.

Affected versions of this package are vulnerable to Uncontrolled Recursion through the image optimization feature. An attacker can cause excessive CPU consumption by exploiting this vulnerability.

Workaround

Ensure that the `next.config.js` file has either `images.unoptimized`, `images.loader` or `images.loaderFile` assigned.

Remediation

Upgrade `next` to version 14.2.7, 15.0.0-canary.109 or higher.

References

- GitHub Commit

More about this vulnerability

HIGH SEVERITY

Missing Authorization

- Package Manager: npm
- Vulnerable module: next
- Introduced through: nextly-template@2.0.0 and next@14.2.3

Detailed paths

- *Introduced through*: nextly-template@2.0.0 › next@14.2.3

Overview

next is a react framework.

Affected versions of this package are vulnerable to Missing Authorization when using pathname-based checks in middleware for authorization decisions. If i18n configuration is not configured, an attacker can get unintended access to pages one level under the application's root directory.

e.g. `https://example.com/foo` is accessible. `https://example.com/` and `https://example.com/foo/bar` are not.

Note:

Only self-hosted applications are vulnerable. The vulnerability has been fixed by Vercel on the server side.

Remediation

Upgrade `next` to version 14.2.15 or higher.

References

- GitHub Commit

More about this vulnerability

MEDIUM SEVERITY

Allocation of Resources Without Limits or Throttling

- Package Manager: npm
- Vulnerable module: next
- Introduced through: nextly-template@2.0.0 and next@14.2.3

Detailed paths

- *Introduced through*: nextly-template@2.0.0 › next@14.2.3

Overview

next is a react framework.

Affected versions of this package are vulnerable to Allocation of Resources Without Limits or Throttling through the Server Actions process. An attacker can cause the server to hang by constructing requests that leave Server-Actions requests pending until the hosting provider terminates the function execution.

Note:

This is only exploitable if there are no protections against long-running Server Action invocations.

Remediation

Upgrade `next` to version 13.5.8, 14.2.21, 15.1.2 or higher.

References

- GitHub Commit
- GitHub Commit

More about this vulnerability

MEDIUM SEVERITY

Improper Input Validation

- Package Manager: npm
- Vulnerable module: nanoid
- Introduced through: nextly-template@2.0.0, next@14.2.3 and others

Detailed paths

- *Introduced through*: nextly-template@2.0.0 › next@14.2.3 › postcss@8.4.31 › nanoid@3.3.7

Overview

Affected versions of this package are vulnerable to Improper Input Validation due to the mishandling of fractional values in the `nanoid` function. By

exploiting this vulnerability, an attacker can achieve an infinite loop.

Remediation

Upgrade `nanoid` to version 3.3.8, 5.0.9 or higher.

References

- GitHub Commit
- GitHub PR
- GitHub Release

More about this vulnerability