Authorization Bypass in Next.js Middleware

Critical **jackwilson323** published **GHSA-f82v-jwr5-mffw** 2 days ago

Package	Affected versions	Patched versions
next (npm)	> 11.1.4 <=13.5.6	None
	>14.0 <14.2.25	14.2.25
	>15.0 <15.2.3	15.2.3

Description

Impact

It is possible to bypass authorization checks within a Next.js application, if the authorization check occurs in middleware.

Patches

- For Next.js 15.x, this issue is fixed in `15.2.3`
- For Next.js 14.x, this issue is fixed in `14.2.25`
- For Next.js versions `11.1.4` thru `13.5.6` we recommend consulting the below workaround.

Note: Next.js deployments hosted on Vercel are automatically protected against this vulnerability.

Workaround

If patching to a safe version is infeasible, we recommend that you prevent external user requests which contain the `x-middleware-subrequest` header from reaching your Next.js application.

Credits

- Allam Rachid (zhero;)

Severity

Critical 9.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2025-29927

Weaknesses

CWE-285

Credits

cold-try Reporter

- Allam Yasser (inzo_)