# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 24/03/2025
**Tema:** Alerta 2025-24  Falla Crítica en Next.js: Vulnerabilidad Permite Evasión de Autorización
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

Paquete: Next.js (npm)

Versiones Vulnerables:

- 11.1.4 y < 12.3.5
- 14.0 y < 14.2.25
- 15.0 y < 15.2.3
- = 13.0.0 y < 13.5.9

## Descripción

Se ha identificado una falla de seguridad crítica en el framework **Next.js**, específicamente en su implementación de **middleware**, lo que podría permitir a atacantes eludir verificaciones de autorización en determinadas condiciones. La vulnerabilidad, catalogada como **CVE-2025-29927**, posee una **puntuación CVSS de 9.1/10**.

Dicha vulnerabilidad indica un alto riesgo de explotación. El problema radica en la manipulación del encabezado interno **x-middleware-subrequest**, el cual Next.js utiliza para evitar bucles infinitos en solicitudes recursivas. Un atacante podría aprovechar esta debilidad para omitir la ejecución del middleware, permitiéndole eludir validaciones críticas, como la verificación de cookies de autorización, antes de acceder a rutas protegidas.

Esta vulnerabilidad permite a los atacantes evitar los controles de autorización del **middleware de Next.js**, lo que podría facilitar el acceso a contenido restringido, como páginas administrativas o recursos exclusivos para usuarios con privilegios elevados. Dado que el middleware se ejecuta antes de que las rutas coincidan y el contenido en caché sea servido, su omisión representa un riesgo grave para la seguridad de las aplicaciones afectadas.

## Mitigación

Si no es posible aplicar una actualización, se recomienda **bloquear las solicitudes externas** que contengan el encabezado **x-middleware-subrequest** para evitar la explotación de esta vulnerabilidad en su aplicación Next.js.

## Solución

Se recomienda actualizar Next.js a las siguientes versiones seguras:

- Next.js 15.x: Actualizar a 15.2.3
- Next.js 14.x: Actualizar a 14.2.25
- Next.js 13.x: Actualizar a 13.5.9
- Next.js 12.x: Actualizar a 12.3.5
- Next.js 11.x: Aplicar la solución alternativa indicada a continuación.

https://nextjs.org/docs/app/building-your-application/upgrading/version-14

## Información adicional:

- https://github.com/vercel/next.js/security/advisories/GHSA-f82v-jwr5-mffw
- https://thehackernews.com/2025/03/critical-nextjs-vulnerability-allows.html
- https://securityonline.info/urgent-patch-your-next-js-for-authorization-bypass-cve-2025-29927/
- https://zhero-web-sec.github.io/research-and-things/nextjs-and-the-corrupt-middleware