Boletín de alerta

Boletín Nro.: 46
Fecha de publicación: 15/04/2026
Tema: Alerta 2026-36 Nueva vulnerabilidad crítica en Axios permite compromiso de entornos cloud
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Axios (npm axios): Todas las versiones anteriores a 1.15.0 (incluye ramas 0.x e 1.x)

Descripción

Se ha reportado una nueva vulnerabilidad crítica en Axios, identificada como **CVE-2026-40175 con un score de 10**, que afecta a versiones anteriores a **Axios 1.15.0**. Esta falla puede permitir a un atacante obtener acceso a entornos cloud e incluso lograr ejecución remota de código (RCE) cuando se combina con servicios y configuraciones específicas, por lo que se la considera de severidad crítica.

Axios es una **librería JavaScript de cliente HTTP basada en promesas** que se utiliza para hacer peticiones HTTP tanto desde el navegador como desde aplicaciones Node.js. Suele estar presente en aplicaciones web y servicios backend que consumen APIs REST, especialmente en ecosistemas como React, Vue o Node.js

En este caso no se trata de paquetes maliciosos publicados en npm como en el incidente anterior, sino de una vulnerabilidad en el propio diseño/implementación de Axios. El problema se explota manipulando cabeceras HTTP construidas a partir de datos no confiables, lo que posibilita inyectar valores y forzar peticiones del servidor hacia endpoints controlados por el atacante (por ejemplo, servicios internos o metadatos cloud). En determinados escenarios, esto puede derivar en acceso a credenciales, tokens de servicios cloud o RCE a través de servicios que procesan esas peticiones.

La solución recomendada es actualizar Axios a la versión **1.15.0 o superior**, donde los mantenedores han corregido esta vulnerabilidad endureciendo el manejo de cabeceras y las rutas de código afectadas. Se recomienda a los administradores y equipos de desarrollo identificar proyectos que dependan de Axios (tanto directas como transitivas), actualizar las dependencias en los archivos de configuración (package.json/lockfiles) y desplegar nuevamente los servicios afectados, priorizando aquellos que tengan exposición a Internet o acceso a recursos cloud sensibles.

Solución:

Se recomienda actualizar Axios a la versión **1.15.0 o superior**, donde se ha corregido la vulnerabilidad CVE-2026-40175, asegurando que tanto las dependencias directas como transitivas se actualicen en los archivos package.json y los correspondientes lockfiles (por ejemplo, package-lock.json o yarn.lock).

En el siguiente enlace encontrará información al respecto de le paquete afectado:

- https://www.npmjs.com/package/axios

Producto	Versiones afectadas	Versión segura recomendada
Axios (npm axios)	Todas las versiones anteriores a 1.15.0 (incluye ramas 0.x e 1.x)	1.15.0 o superior

Tras la actualización, se debe reconstruir y desplegar nuevamente las aplicaciones afectadas, revisando especialmente aquellos servicios que construyen cabeceras HTTP a partir de datos no confiables y los que tienen acceso a recursos cloud sensibles (como metadatos de instancias o servicios internos), así como aplicar buenas prácticas de hardening en la red y en los entornos cloud para limitar el impacto de posibles explotaciones residuales.

Información adicional:

- https://nvd.nist.gov/vuln/detail/CVE-2026-40175
- https://securityonline.info/axios-vulnerability-cve-2026-40175-cloud-takeover-rce/
- https://www.npmjs.com/package/axios