Boletín de alerta

Boletín Nro.: 31
Fecha de publicación: 31/03/2026
Tema: Alerta 2026-31 Paquetes maliciosos en Axios publicados por NPM
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Las versiones maliciosas de axios comprometidas en el ataque de cadena de suministro son **1.14.1** y **0.30.4**.

Descripción

Un sofisticado ataque a la cadena de suministro ha tenido como objetivo a Axios, uno de los clientes HTTP más utilizados dentro del ecosistema JavaScript, mediante la introducción de una dependencia transitiva maliciosa en el registro oficial de npm.

Las versiones afetadas fueron **1.14.1** y **0.30.4**. y las mismas se han publicado el 30 de marzo de 2026 mediante la cuenta npm comprometida del mantenedor principal «jasonsaayman», quien cambió su email a uno de ProtonMail controlado por el atacante.

Inyectan una dependencia oculta «plain-crypto-js@4.2.1», que ejecuta un script postinstall para desplegar un RAT (Remote Access Trojan) multiplataforma en macOS, Windows y Linux.

El malware contacta un servidor C2, descarga payloads secundarios, se ejecuta y se auto-elimina, reemplazando su package.json para evadir detección.

Mitigación:

Las librerías comprometidas afectan a quienes ejecutaron «npm install» en esas versiones durante ~2 horas; npm las removió después.

La recomendación es: reviertir axios a 1.14.0 ó a 0.30.3, revisa lockfiles/package-lock.json, cambia credenciales y escanea sistemas.

Comandos Básicos:

```
# Ver versión instalada de axios
npm list axios
# Buscar específicamente las versiones comprometidas
npm list axios 2>/dev/null | grep -E "1\.14\.1|0\.30\.4"
# Buscar en package-lock.json (NPM)
grep -A1 '"axios"' package-lock.json | grep -E "1\.14\.1|0\.30\.4"
# Buscar en yarn.lock (Yarn)
grep -E 'axios@' yarn.lock | grep -E "1\.14\.1|0\.30\.4"
# Buscar el paquete RAT oculto
ls node_modules | grep plain-crypto-js || echo "No encontrado"
# Verificar postinstall scripts sospechosos
grep -r "postinstall" node_modules/axios/ 2>/dev/null || echo "Sin scripts postinstall"
```

Monitorea repositorios y usa herramientas como Snyk o npm audit para vulnerabilidades futuras.

Paquete comprometido	Version	Dependencia maliciosa
Axios	1.14.1	plain-crypto-js@4.2.1
Axios	0.30.4	plain-crypto-js@4.2.1
plain-crypto-js	4.2.1	Primary Malicious Payload

A continuación listamos, algunos de los paquetes mas conocidos que dependen de **axios**, es importante revisar el package-lock.json :

- auth0
- alchemy-sdk
- @tavily/core
- @slack/web-api
- aws-crt
- contentful-management
- @coinbase/cdp-sdk
- postmark –
- @sap-cloud-sdk/core
- fastmcp
- mcp-proxy
- swagger-client
- wagmi
- gatsby
- wait-on
- posthog-node

Información adicional:

- https://cybersecuritynews.com/axios-npm-packages-compromised/