Boletín de alerta

Boletín Nro.:
Fecha de publicación: 25/03/2025
Tema: Alerta 2025-25 Ataque a la cadena de suministro compromete repositorios en GitHub
Traffic Light Protocol (TLP): Amber

Descripción

Se ha identificado un ataque a la cadena de suministro en GitHub Actions, que inició como un ataque dirigido a un proyecto de código abierto de Coinbase y posteriormente se amplió a otros repositorios. La vulnerabilidad afecta la acción «tj-actions/changed-files», permitiendo la inyección de código malicioso para filtrar información confidencial de los repositorios que ejecutaban flujos de trabajo afectados.

Este incidente fue revelado el 14 de marzo de 2025, cuando se detectó la manipulación de «tj-actions/changed-files», lo que llevó a la asignación del identificador CVE-2025-30066 (CVSS 8.6). Se estima que 218 repositorios de GitHub expusieron credenciales de servicios como DockerHub, npm y AWS, así como tokens de acceso de instalación de GitHub.

Además, se identificó que la acción «reviewdog/action-setup», de la cual «tj-actions/changed-files» depende indirectamente, también fue comprometida con una carga maliciosa similar. Esta brecha se registró como CVE-2025-30154 (CVSS 8.6) y permitió a los atacantes obtener un Token de Acceso Personal (PAT), lo que facilitó la modificación del código fuente del repositorio afectado y amplificó el impacto en la comunidad

Solución

- Actualizar a versiones seguras de las acciones afectadas.
- Revisar los flujos de CI/CD en busca de configuraciones vulnerables.
- Rotar credenciales comprometidas y reforzar la seguridad de los secretos en GitHub.
- Restringir el uso del encabezado x-middleware-subrequest en flujos de trabajo de GitHub.

Información adicional:
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://thehackernews.com/2025/03/github-supply-chain-breach-coinbase.html
- https://fluidattacks.com/blog/tj-actions-changed-files-vulnerability/