# Security Advisory – Supply Chain Attack on reviewdog GitHub Actions

## Resumen del incidente

El issue #2079 en el repositorio reviewdog informa sobre un ataque a la cadena de suministro que afectó la acción GitHub reviewdog/action-setup@v1. Este ataque permitió sobrescribir la etiqueta @v1 con código malicioso, lo que potencialmente expuso secretos de repositorios que usaban esta acción durante un periodo específico.

## Periodo comprometido

El ataque ocurrió el 11 de marzo de 2025 entre las 18:42 y 20:31 UTC.

## Cómo ocurrió

El atacante utilizó un token de acceso personal (PAT) comprometido de un contribuidor legítimo de reviewdog. Utilizando este PAT, realizaron un git push que sobrescribió la etiqueta v1. Esta actividad no aparece en los logs públicos, pero fue rastreada con ayuda del soporte de GitHub mediante git reflog y auditoría de tokens.

## Acciones tomadas

- Desactivación del sistema de invitaciones automáticas

- Revocación de accesos de escritura a la mayoría de los miembros

- Fijación de versiones de acciones por SHA en lugar de etiquetas

- Rotación y eliminación de tokens comprometidos

## Recomendaciones para usuarios

- Evita usar etiquetas como @v1. Usa commit SHAs en su lugar

- Verifica si tu repositorio estuvo comprometido usando herramientas proporcionadas por Wiz

- Considera usar el binario de reviewdog directamente para mayor seguridad

## Recursos adicionales

- Blog de Wiz: https://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup

- Informe de Unit42 (Palo Alto Networks): https://unit42.paloaltonetworks.com/github-actions-supply-chain-attack/

- Commit malicioso: https://gist.github.com/haya14busa/1a6072b647e829ace5382f36b9ada60a

## Conclusión

Este incidente demuestra los riesgos de seguridad asociados a GitHub Actions cuando se usan etiquetas flotantes como @v1. Es fundamental fijar versiones por SHA, limitar el acceso de colaboradores y auditar regularmente el uso de tokens.