Boletín de alerta

Boletín Nro.:
Fecha de publicación: 27/03/2026
Tema: Alerta 2026-30 Ataque cadena de suministro Checkmarx
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Checkmarx GitHub Actions:** `ast-github-action` y `kics-github-action`.
- **Extensiones OpenVSX:** `cx-dev-assist` (v1.7.0) y `ast-results` (v2.53.0).
- **Versiones:** Tags de GitHub Action publicados entre las 12:58 y 16:50 UTC del 23 de marzo de 2026.

Descripción

Recientemente se ha identificado un compromiso crítico en la cadena de suministro de Checkmarx, un proveedor líder en soluciones de pruebas de seguridad de aplicaciones (AST). Este incidente forma parte de una campaña a gran escala atribuida al actor de amenazas TeamPCP, que también ha impactado otros proyectos de código abierto como Trivy y LiteLLM.

El ataque se originó mediante el compromiso de la cuenta de servicio cx-plugins-releases en GitHub, lo que permitió al atacante inyectar cargas útiles maliciosas en los flujos de trabajo de CI/CD mediante el uso de «imposter commits» y la manipulación de etiquetas (tags).

El malware inyectado funciona como un credential stealer diseñado para recolectar variables de entorno, claves SSH y tokens de proveedores de nube (AWS, Azure, GCP). Los datos recolectados se cifran y se exfiltran mediante peticiones POST hacia el dominio malicioso checkmarx[.]zone. El vector de ejecución utiliza gestores de paquetes JavaScript comunes como npx, bunx o pnpx para ejecutar el código malicioso durante los procesos de integración continua.

Solución y mitigaciones:

Tras su detección, Checkmarx elimino los artefactos maliciosos, se fijaron los flujos de trabajo a hashes SHA de confirmación seguros y verificados, se revocó y roto todas las credenciales expuestas, se bloqueó el acceso saliente al dominio controlado por el atacante y se revisaron entornos en busca de cualquier indicio de una mayor vulneración.

Si se descargó y ejecutó alguna de las extensiones mencionadas anteriormente desde el registro de Open VSX, su organización podría verse afectada y se recomienda tomar las siguientes acciones:

1. Remover los componentes maliciosos
2. Revocar y rotar credenciales
3. Bloquear infraestructura maliciosa
4. Investigar accesos no autorizados

Información adicional:

- https://checkmarx.com/blog/checkmarx-security-update/
- https://www.wiz.io/blog/teampcp-attack-kics-github-action
- https://socradar.io/blog/teampcp-checkmarx-github-actions-attack/
- https://www.sysdig.com/blog/teampcp-expands-supply-chain-compromise-spreads-from-trivy-to-checkmarx-github-actions