Checkmarx ha informado que su investigación en curso, vinculada al incidente de seguridad en la cadena de suministro, ha descubierto que un grupo de ciberdelincuentes publicó información relacionada con la empresa en la dark web.

"Con base en la evidencia disponible actualmente, creemos que estos datos provienen del repositorio de GitHub de Checkmarx, y que el acceso a dicho repositorio se logró mediante el ataque inicial a la cadena de suministro ocurrido el 23 de marzo de 2026," señaló la compañía de seguridad israelí.

También subrayó que el repositorio de GitHub se gestiona de forma independiente respecto a su entorno de producción para clientes, añadiendo que en él no se almacena información de clientes. Checkmarx indicó que su investigación forense sigue en marcha y que trabaja activamente para confirmar la naturaleza y el alcance de los datos publicados.

Además, la empresa afirmó que ha restringido el acceso al repositorio de GitHub afectado como parte de sus acciones de respuesta al incidente.

"Si determinamos que la información de clientes estuvo implicada en este incidente, notificaremos de inmediato a los clientes y a todas las partes pertinentes," indicó.

Este desarrollo se produce después de que Dark Web Informer compartiera en una publicación en X que el grupo cibercriminal LAPSUS$ afirmó haber añadido tres víctimas a su sitio de filtraciones de datos, entre ellas Checkmarx. Según el listado, la información incluye código fuente, base de datos de empleados, claves API y credenciales de MongoDB/MySQL.

Checkmarx sufrió una brecha a finales del mes pasado tras el ataque a la cadena de suministro de Trivy, lo que provocó la manipulación de dos de sus flujos de trabajo de GitHub Actions y de dos complementos distribuidos a través del marketplace Open VSX, con el fin de introducir un ladrón de credenciales capaz de recolectar una amplia variedad de secretos de desarrolladores. El actor de amenazas conocido como TeamPCP se atribuyó la autoría del ataque.

La semana pasada, se sospecha que este grupo con motivaciones financieras comprometió la imagen Docker de KICS de Checkmarx, junto con dos extensiones de VS Code y un flujo de trabajo de GitHub Actions con un malware similar diseñado para robar credenciales. Esto, a su vez, provocó un efecto en cadena que derivó en la breve vulneración del paquete npm de Bitwarden CLI.