Se han descubierto tres fallos de seguridad en el gestor de dependencias CocoaPods para proyectos Cocoa en Swift y Objective-C, los cuales podrían ser explotados para llevar a cabo ataques a la cadena de suministro de software, poniendo a los usuarios en grave riesgo.

Las vulnerabilidades permiten que «*cualquier actor malicioso pueda reclamar la propiedad de miles de pods no reclamados e insertar código malicioso en muchas de las aplicaciones más populares de iOS y macOS,*» según indicaron los investigadores de seguridad de la información de E.V.A., Reef Spektor y Eran Vaknin, en un informe publicado hoy.

La empresa israelí de seguridad de aplicaciones informó que los tres problemas han sido corregidos por CocoaPods desde octubre de 2023. Además, se reiniciaron todas las sesiones de usuario en respuesta a las revelaciones.

Una de las vulnerabilidades es CVE-2024-38368 (puntuación CVSS: 9.3), que permite a un atacante abusar del proceso «*Reclama tus Pods*» y tomar el control de un paquete, lo que les permite modificar el código fuente e introducir cambios maliciosos. Sin embargo, esto requería que todos los mantenedores anteriores hubieran sido eliminados del proyecto.

El origen del problema se remonta a 2014, cuando una migración al servidor Trunk dejó miles de paquetes con propietarios desconocidos (o no reclamados), permitiendo a un atacante usar una API pública para reclamar pods y una dirección de correo electrónico que estaba disponible en el código fuente de CocoaPods («unclaimed-pods@cocoapods.org») para tomar el control.

El segundo error es aún más grave (CVE-2024-38366, puntuación CVSS: 10.0) y explota un flujo de verificación de correo electrónico inseguro para ejecutar código arbitrario en el servidor Trunk, que luego podría usarse para manipular o reemplazar los paquetes.

También se detectó en el servicio un segundo problema en el componente de verificación de direcciones de correo electrónico (CVE-2024-38367, puntuación CVSS: 8.2) que podría inducir a un destinatario a hacer clic en un enlace de verificación aparentemente inofensivo, cuando

en realidad redirige la solicitud a un dominio controlado por un atacante para obtener acceso a los tokens de sesión de un desarrollador.

Para empeorar la situación, esto puede convertirse en un ataque de toma de control de cuenta sin necesidad de interacción del usuario al falsificar un encabezado HTTP, es decir, modificando el campo del encabezado X-Forwarded-Host, y aprovechando herramientas de seguridad de correo electrónico mal configuradas.

> *«Hemos encontrado que casi todos los propietarios de pods están registrados con el correo electrónico de su organización en el servidor Trunk, lo que los hace vulnerables a nuestra vulnerabilidad de toma de control sin necesidad de interacción del usuario,»* señalaron los investigadores.

Esta no es la primera vez que CocoaPods está bajo observación. En marzo de 2023, Checkmarx reveló que un subdominio abandonado asociado con el gestor de dependencias («cdn2.cocoapods[.]org») podría haber sido secuestrado por un adversario a través de GitHub Pages con el objetivo de alojar sus cargas maliciosas.