Han salido a la luz detalles sobre una vulnerabilidad crítica de seguridad —ya corregida— en el popular paquete de npm "@react-native-community/cli", la cual podría haber sido explotada para ejecutar comandos maliciosos del sistema operativo (OS) bajo ciertas condiciones.

"La vulnerabilidad permite que atacantes remotos y no autenticados ejecuten fácilmente comandos arbitrarios del sistema operativo en la máquina que ejecuta el servidor de desarrollo de react-native-community/cli, lo que representa un riesgo significativo para los desarrolladores," señaló Or Peles, investigador senior de seguridad en JFrog.

La vulnerabilidad, identificada como CVE-2025-11953, tiene una puntuación CVSS de 9.8 sobre un máximo de 10.0, lo que indica una gravedad crítica. También afecta las versiones del paquete "@react-native-community/cli-server-api" desde la 4.8.0 hasta la 20.0.0-alpha.2, y fue corregida en la versión 20.0.0, publicada a inicios del mes pasado.

Este paquete de herramientas de línea de comandos, mantenido por Meta, permite a los desarrolladores crear aplicaciones móviles con React Native, y recibe aproximadamente entre 1.5 y 2 millones de descargas por semana.

Según la empresa especializada en seguridad de la cadena de suministro de software, la vulnerabilidad proviene del hecho de que el servidor de desarrollo Metro, utilizado por React Native para compilar el código y los recursos JavaScript, se vincula por defecto a interfaces externas (en lugar de localhost) y expone un endpoint "/open-url" susceptible a inyección de comandos del sistema operativo.

"El endpoint '/open-url' del servidor maneja una solicitud POST que incluye un valor proporcionado por el usuario, el cual se pasa a la función insegura open() del paquete open de npm, lo que provoca la ejecución de comandos del sistema operativo," explicó Peles.

Como consecuencia, un atacante en la red sin autenticación podría explotar la falla enviando una solicitud POST especialmente diseñada al servidor, lo que le permitiría ejecutar comandos arbitrarios. En Windows, los atacantes pueden ejecutar comandos del shell con

argumentos totalmente controlados, mientras que en Linux y macOS el fallo puede utilizarse para ejecutar binarios arbitrarios con un control limitado de parámetros.

Aunque el problema ya ha sido solucionado, los desarrolladores que utilizan React Native con frameworks que no dependen de Metro como servidor de desarrollo no se ven afectados.

"Esta vulnerabilidad de día cero es especialmente peligrosa debido a su facilidad de explotación, la ausencia de requisitos de autenticación y su amplia superficie de ataque," advirtió Peles. *"También pone de manifiesto los riesgos críticos ocultos en el código de terceros."*

"Para los equipos de desarrollo y seguridad, esto resalta la necesidad de contar con escaneos de seguridad automatizados y exhaustivos a lo largo de toda la cadena de suministro de software, con el fin de garantizar que las vulnerabilidades fácilmente explotables sean corregidas antes de afectar a la organización."