Vulnerabilidades graves descubiertas en las populares extensiones de Visual Studio Code, podrían permitir a los atacantes comprometer las máquinas locales, así como los sistemas de construcción e implementación a través del entorno de desarrollo integrado (IDE) de un desarrollador.

Las extensiones vulnerables podrían explotarse para ejecutar código arbitrario en el sistema de un desarrollador de forma remota, lo que en última instancia podría allanar el camino para los ataques a la cadena de suministro.

Algunas de las extensiones en cuestión son LaTeX Workshop, Rainbow Fart, Open in Default Browser y Instant Markdown, todas las cuales acumulan alrededor de dos millones de instalaciones entre ellas.

> *«Las máquinas de desarrollo suelen tener credenciales importantes, lo que les permite interactuar con muchas partes del producto. La filtración de la clave privada de un desarrollador puede permitir que una parte interesada malintencionada clone partes importantes del código base o incluso se conecte a servidores de producción»*, dijeron los investigadores de Synk.

Las extensiones de VS Code, como los complementos del navegador, permiten a los desarrolladores aumentar el editor de código fuente de Visual Studio Code de Microsoft, con características adicionales como lenguajes de programación y depuradores relevantes para sus flujos de trabajo de desarrollo. VS Code es utilizado por 14 millones de usuarios activos, lo que lo convierte en una enorme superficie de ataque.

Los escenarios de ataques ideados por Synk se basan en la posibilidad de que las extensiones instaladas puedan ser abusadas como un vector de ataques a la cadena de suministro al explotar las debilidades en los complementos para ingresar a un sistema de

desarrollo de forma efectiva. A tal efecto, los investigadores examinaron las extensiones de VS Code que tenían implementaciones vulnerables de servidores web locales.

En un caso destacado por los investigadores de Synk, una vulnerabilidad de recorrido de ruta identificada en Instant Markdown podría ser aprovechada por un mal actor con acceso al servidor web local (conocido como localhost) para recuperar cualquier archivo alojado en la máquina simplemente engañando a un desarrollador para que haga clic en un archivo malicioso.

Como demostración de prueba de concepto (PoC), los investigadores demostraron que era posible explotar esta falla para robar claves SSH de un desarrollador que ejecuta VS Code y tiene Instant Markdown o Open in Default Browser instalado en el IDE. LaTeX Workshop, por otro lado, se encontró susceptible a una vulnerabilidad de inyección de comandos debido a una entrada no desinfectada que podría explotarse para ejecutar cargas útiles maliciosas.

Finalmente, se determinó que una extensión llamada Rainbow Fart tiene una vulnerabilidad de deslizamiento de cremallera, que permite a un adversario sobrescribir archivos arbitrarios en la máquina de una víctima y obtener la ejecución remota de código. En un ataque formulado por los investigadores, se envió un archivo ZIP especialmente diseñado por medio de un punto final «import-voice-package» utilizado por el complemento y se escribió en una ubicación que está fuera del directorio de trabajo de la extensión.

> *«Este ataque podría usarse para sobrescribir archivos como «.bashrc» y obtener la ejecución remota de código eventualmente»,* dijeron los investigadores.

Aunque las fallas en las extensiones se abordaron desde entonces, los hallazgos son importantes a la luz de una serie de incidentes de seguridad que muestran cómo los desarrolladores han surgido como un objetivo de ataque lucrativo, con actores de amenazas

que liberan una variedad de malware para comprometer las herramientas y entornos de desarrollo para otras campañas.

> *«Lo que ha sido claro para las dependencias de terceros también lo está ahora para los complementos IDE: introducen un riesgo inherente a una aplicación. Son potencialmente peligrosos tanto por sus piezas de código escritas personalizadas como por las dependencias sobre las que se basan. Lo que se ha demostrado aquí para VS Code también podría ser aplicable a otros IDE, lo que significa que instalar extensiones o complementos a ciegas no es seguro (nunca lo ha sido)»*, dijeron los investigadores de Synk, Raul Onitza-Klugman y Kirill Efimov.