Investigadores de ciberseguridad han revelado múltiples vulnerabilidades en cuatro extensiones populares de Microsoft Visual Studio Code (VS Code) que, si se explotan con éxito, podrían permitir a actores maliciosos robar archivos locales y ejecutar código de forma remota.

Las extensiones afectadas, que en conjunto superan los 125 millones de instalaciones, son Live Server, Code Runner, Markdown Preview Enhanced y Microsoft Live Preview.

«Nuestra investigación demuestra que un atacante solo necesita una extensión maliciosa, o una única vulnerabilidad dentro de una extensión, para desplazarse lateralmente y comprometer organizaciones enteras», señalaron los investigadores de OX Security Moshe Siman Tov Bustan y Nir Zadok en un informe.

Los detalles de las vulnerabilidades son los siguientes:

- CVE-2025-65717 (Puntuación CVSS: 9.1) – Una falla en Live Server que posibilita la exfiltración de archivos locales al inducir al desarrollador a visitar un sitio web malicioso mientras la extensión está activa. Esto provoca que código JavaScript incrustado en la página explore y extraiga archivos desde el servidor HTTP de desarrollo local que opera en localhost:5500, enviándolos posteriormente a un dominio controlado por el atacante. (Permanece sin parche)
- CVE-2025-65716 (Puntuación CVSS: 8.8) – Una vulnerabilidad en Markdown Preview Enhanced que permite ejecutar código JavaScript arbitrario mediante la carga de un archivo markdown (.md) manipulado, facilitando la enumeración de puertos locales y la exfiltración de información hacia un dominio bajo control del atacante. (Permanece sin parche)
- CVE-2025-65715 (Puntuación CVSS: 7.8) – Una debilidad en Code Runner que posibilita la ejecución de código arbitrario si el atacante logra convencer al usuario, mediante phishing o ingeniería social, de modificar el archivo «settings.json». (Permanece sin parche)
- Una vulnerabilidad en Microsoft Live Preview permite acceder a archivos sensibles en el equipo del desarrollador al engañar a la víctima para que visite un sitio web

malicioso mientras la extensión está en ejecución. Esto habilita solicitudes JavaScript especialmente diseñadas contra el localhost para enumerar y extraer archivos confidenciales. (Sin CVE asignado; corregida silenciosamente por Microsoft en la versión 0.4.16 lanzada en septiembre de 2025)

Para proteger el entorno de desarrollo, es fundamental evitar aplicar configuraciones no confiables, deshabilitar o desinstalar extensiones innecesarias, reforzar la red local mediante un firewall que limite las conexiones entrantes y salientes, actualizar periódicamente las extensiones y desactivar los servicios basados en localhost cuando no estén en uso.

«Las extensiones mal desarrolladas, excesivamente permisivas o directamente maliciosas pueden ejecutar código, modificar archivos y permitir que atacantes tomen el control de una máquina y extraigan información», indicó OX Security. «Mantener extensiones vulnerables instaladas en un equipo representa una amenaza inmediata para la seguridad de una organización: puede bastar un solo clic o la descarga de un repositorio para comprometerlo todo.»