Los hackers están haciendo esfuerzos activos para explotar una nueva variante de una vulnerabilidad de escalada de privilegios recientemente revelada para ejecutar potencialmente código arbitrario en sistemas completamente parcheados, demostrando una vez más cómo los adversarios se mueven rápidamente para convertir en arma un exploit disponible de forma pública.

Cisco Talos reveló que *«detectó muestras de malware en la naturaleza que intentan aprovechar esta vulnerabilidad».*

Rastreada como CVE-2021-41379 y descubierta por el investigador de seguridad Abdelhamid Naceri, la vulnerabilidad de elevación de privilegios que afecta al componente de software Windows Installer, se resolvió originalmente como parte de las actualizaciones del martes de parches de Microsoft para noviembre de 2021.

Sin embargo, en un caso de parche insuficiente, Naceri descubrió que no solo era posible omitir la solución implementada por Microsoft, sino también lograr una escalada de privilegios local a través de un error de día cero recién descubierto.

El exploit de prueba de concepto (PoC), denominado «InstallerFileTakeOver«, funciona sobrescribiendo la lista de control de acceso discrecional (DACL) para Microsoft Edge Elevation Service, para reemplazar cualquier archivo ejecutable en el sistema con un archivo de instalación MSI, lo que permite que un atacante ejecute código con privilegios de SISTEMA.

Un atacante con privilegios de administrador podría abusar del acceso para obtener un control total sobre el sistema comprometido, incluida la capacidad de descargar software adicional y modificar, eliminar o exfiltrar información confidencial almacenada en la máquina.

> *«Puedo confirmar que esto funciona, local priv esc. probado en Windows 10 20H2 y Windows 11. El parche anterior que MS emitió no solucionó el problema correctamente»,* dijo el investigador de seguridad Kevin Beaumont.

Naceri dijo que la última variante de CVE-2021-41379 es *«más poderosa que la original»* y que el mejor curso de acción sería esperar a que Microsoft lance un parche de seguridad para el problema *«debido a la complejidad de esta vulnerabilidad».*