Se ha revelado una vulnerabilidad en la función Attended Sysupgrade (ASU) de OpenWrt que, si se explota con éxito, podría haberse utilizado para distribuir paquetes de firmware maliciosos.

La vulnerabilidad, identificada como CVE-2024-54143, tiene una puntuación CVSS de 9.3 sobre 10, lo que indica una gravedad crítica. El investigador de Flatt Security, RyotaK, ha sido reconocido por descubrir y reportar la falla el 4 de diciembre de 2024. El problema se ha corregido en la versión 920c8a1 de ASU.

> *«Debido a la combinación de la inyección de comandos en la imagen del generador de imágenes (imagebuilder) y el hash SHA-256 truncado incluido en el hash de la solicitud de compilación, un atacante puede contaminar la imagen legítima proporcionando una lista de paquetes que provoque una colisión de hashes»,* señalaron los mantenedores del proyecto en una alerta.

OpenWrt es un sistema operativo basado en Linux de código abierto popular para routers, puertas de enlace residenciales y otros dispositivos integrados que gestionan tráfico de red.

La explotación exitosa de esta vulnerabilidad podría permitir a un actor malicioso inyectar comandos arbitrarios en el proceso de compilación, lo que resultaría en la creación de imágenes de firmware maliciosas firmadas con la clave legítima de compilación.

Aún más grave, una colisión de hash SHA-256 de 12 caracteres asociada con la clave de compilación podría ser utilizada para servir una imagen maliciosa previamente creada en lugar de una legítima, representando un grave riesgo para la cadena de suministro de los usuarios finales.

> *«Un atacante necesita la capacidad de enviar solicitudes de compilación que incluyan listas de paquetes manipuladas. No se requiere autenticación para explotar estas vulnerabilidades. Al inyectar comandos y provocar colisiones de*

> *hash, el atacante puede hacer que solicitudes de compilación legítimas reciban una imagen maliciosa generada previamente»,* señaló OpenWrt.

RyotaK, quien proporcionó un análisis técnico del error, dijo que no se sabe si la vulnerabilidad fue explotada activamente, ya que ha *«existido durante un tiempo».* Se recomienda a los usuarios actualizar a la última versión lo antes posible para protegerse contra posibles amenazas.