



Investigadores descubren una vulnerabilidad de inyección de comandos en el conjunto de pruebas de Wi-Fi Alliance

Una vulnerabilidad en la Wi-Fi Test Suite podría permitir que atacantes locales sin autenticación ejecuten código arbitrario con privilegios elevados.

El Centro de Coordinación CERT (CERT/CC) informó sobre la vulnerabilidad, identificada como CVE-2024-41992, y señaló que el código afectado de la Wi-Fi Alliance se encuentra implementado en routers Arcadyan FMIMG51AX000J.

«Esta falla permite que un atacante local no autenticado aproveche la Wi-Fi Test Suite mediante el envío de paquetes especialmente contruidos, lo que posibilita la ejecución de comandos con privilegios de root en los routers comprometidos», [afirmó](#) el CERT/CC en un comunicado emitido el miércoles.

La Wi-Fi Test Suite es una [plataforma integral](#) desarrollada por la Wi-Fi Alliance para automatizar pruebas de componentes y dispositivos Wi-Fi. Aunque algunos componentes de código abierto están [disponibles públicamente](#), el paquete completo solo está accesible para los miembros de la Wi-Fi Alliance.

SSD Secure Disclosure, que publicó [información](#) sobre la falla en agosto de 2024, la describió como un caso de inyección de comandos que podría permitir a un atacante ejecutar comandos con privilegios de root. La vulnerabilidad fue reportada inicialmente a la Wi-Fi Alliance en abril de 2024.

Un investigador independiente, conocido en línea como «fj016», ha sido reconocido por descubrir y [reportar](#) esta vulnerabilidad. El investigador también ha compartido una [prueba de concepto](#) (PoC) para la explotación de la falla.

CERT/CC destacó que la Wi-Fi Test Suite no está diseñada para usarse en entornos de producción, aunque se ha encontrado en despliegues de routers comerciales.

«Un atacante que logre explotar esta vulnerabilidad puede obtener control



Investigadores descubren una vulnerabilidad de inyección de comandos en el conjunto de pruebas de Wi-Fi Alliance

administrativo completo sobre el dispositivo afectado», afirmó CERT/CC.

«Con este nivel de acceso, el atacante puede modificar la configuración del sistema, interrumpir servicios de red críticos o reiniciar el dispositivo por completo. Estas acciones pueden causar interrupciones del servicio, comprometer datos de la red e incluso llevar a una pérdida de servicio para todos los usuarios conectados a la red afectada».

En caso de no haber un parche disponible, se recomienda que los proveedores que hayan integrado la Wi-Fi Test Suite la eliminen de los dispositivos de producción o la actualicen a la versión 9.0 o posterior para reducir el riesgo de explotación.