ALERTA

Vulnerabilidades Críticas en Routers D-Link DIR-846

COLCERT AL-0509-045

TLP:CLEAR

D-Link ha identificado múltiples vulnerabilidades críticas de ejecución de código remoto (RCE) en su modelo de router DIR-846, el cual ya ha sido descontinuado. Estas vulnerabilidades, si son explotadas, podrían permitir a los atacantes tomar el control completo de los dispositivos afectados, lo que representa un riesgo grave para la seguridad de las redes domésticas y empresariales.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

Vulnerabilidades: Las vulnerabilidades encontradas en el DIR-846 permiten a los atacantes remotos ejecutar código arbitrario en el dispositivo, lo que significa que podrían instalar malware, obtener datos o incluso utilizar el router como punto de apoyo para atacar otros dispositivos en la red.

ANÁLISIS

Impacto. Las consecuencias de estas vulnerabilidades son graves y pueden incluir:

- **Pérdida de datos:** Los atacantes podrían robar información sensible almacenada en dispositivos conectados al router.
- **Control remoto de dispositivos:** Los atacantes podrían utilizar el router comprometido para controlar otros dispositivos en la red.

IMPACTO PARA COLOMBIA Y LA REGIÓN

Las vulnerabilidades descubiertas en el router D-Link DIR-846 resaltan la importancia de mantener los dispositivos actualizados y de seguir buenas prácticas de seguridad. Los usuarios deben estar atentos a las alertas de seguridad y tomar las medidas necesarias para proteger sus sistemas.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://securityaffairs.com/168041/security/d-link-dir-846-routers-code-execution-flaws.html
https://cybersecuritynews.com/d-link-declines-to-patch-rce-vulnerabilities/

COLCERT