ALERTA

Dispositivos de red tienen criticas vulnerabilidades

COLCERT AL-1611-058

TLP:CLEAR

Una grave vulnerabilidad de seguridad ha sido descubierta en los módems D-Link DSL6740C, permitiendo a ciberdelincuentes tomar el control total de estos dispositivos sin necesidad de una contraseña.

ELEMENTOS DE INTELIGENCIA DISPONIBLES

A pesar de la gravedad de la situación, D-Link ha decidido no lanzar un parche, ya que el dispositivo ha sido descontinuado. Esto deja a miles de módems vulnerables en todo el mundo expuestos a la opción de ataques cibernéticos.

La vulnerabilidad fue descubierta en el módem D-Link DSL6740C por el investigador de seguridad Chaio-Lin Yu (Steven Meow).

ANÁLISIS

La falla (CVE-2024-11068) permite a los atacantes no autenticados modificar la contraseña de cualquier usuario a través del acceso privilegiado a la API, dándoles control completo sobre los servicios web, SSH y Telnet del módem.

También se reportaron otras dos vulnerabilidades: un problema de recorrido de ruta (CVE-2024-11067) y un error de inyección de comandos del sistema operativo (CVE-2024-11066).

IMPACTO PARA COLOMBIA Y LA REGIÓN

TWCERTCC también ha publicado avisos para otras cuatro vulnerabilidades de inyección de comandos del sistema operativo de alta gravedad (CVE-2024-11062 a CVE-2024-11065) que afectan al mismo dispositivo D-Link.

El gran número de dispositivos vulnerables expuestos es significativo, ya que D-Link ha declarado que no proporcionará ninguna actualización para el dispositivo afectado al final de su vida útil.

NIVEL DE RIESGO

ALTO

FUENTES:

https://securityaffairs.com/170995/iot/cve-2024-10914-d-link-nas-flaw-exploited.html

https://www.securityweek.com/unpatched-flaw-in-legacy-d-link-nas-devices-exploited-days-after-disclosure/

https://supportannouncement.us.dlink.com/

COLCERT