El fabricante taiwanés de equipos de redes D-Link, acordó implementar un *«programa completo de seguridad de software»* para resolver una demanda de la Comisión Federal de Comercio (FTC). en la que se alega que la compañía no tomó las medidas adecuadas para proteger a sus consumidores de los ataques de piratas informáticos.

Su enrutador inalámbrico es la primera línea de defensa contra amenazas potenciales en Internet, por lo que la seguridad es un tema primordial.

Lamentablemente, los enrutadores más utilizados no ofrecen las funciones de seguridad necesarias, por lo que constantemente, se encuentran vulnerables a fallas de seguridad graves, lo que eventualmente permite que los hackers remotos accedan sin autorización a redes y comprometan la seguridad de otros dispositivos conectados.

En los últimos años, la seguridad de las redes inalámbricas ha sido más un tema importante debido a los ataques cibernéticos, además, ganaron popularidad luego del descubrimiento de las vulnerabilidades críticas, como la omisión de autenticación, ejecución remota de código, credenciales de inicio de sesión codificadas y revelación de información en enrutadores fabricados por distintas marcas.

En 2017, la Comisión Federal de Comercio (FTC) de Estados Unidos, presentó una demanda contra D-Link, uno de los fabricantes de enrutadores más populares, por la poca seguridad de sus enrutadores inalámbricos, cámaras IP y otros dispositivos conectados a Internet.

Según la queja de la FTC, D-Link supuestamente falsificó la seguridad de sus productos a sus clientes, no probó adecuadamente sus productos en busca de fallas de seguridad conocidas y fáciles de solucionar, y tampoco pudo proteger los dispositivos cuando se detectaron vulnerabilidades de seguridad.

> *«Los demandados D-Link repetidamente no tomaron medidas razonables de prueba y remediación de software para proteger sus enrutadores y cámaras IP contra fallas de seguridad de software bien conocidas y fácilmente prevenibles. En verdad y de*

> *hecho, los demandados no tomaron medidas razonables para proteger sus productos del acceso no autorizado»,* dice la queja.

En 2015, D-Link también publicó accidentalmente sus claves privadas de firma de código en Internet que podrían haber permitido a los piratas informáticos firmar su malware y evadir la detección.

Ayer, la FTC publicó un acuerdo «amigable» que dice que D-Link debe seguir una planificación de seguridad, un modelo de amenazas, pruebas de vulnerabilidad y remediación antes de que lleguen al mercado sus enrutadores y cámaras IP.

El acuerdo también obliga a la empresa a supervisar sus productos en busca de fallas de seguridad, actualizar el firmware automáticamente y configurar un sistema para aceptar informes de vulnerabilidad de los investigadores de seguridad.

Además, D-Link también acordó realizar auditorías de seguridad de su programa de seguridad de software cada dos años durante los siguientes 10 años, por parte de un asesor independiente aprobado por la FTC.

En un comunicado de prensa, D-Link afirma que la FTC no ha encontrado a la compañía responsable por presuntas violaciones, pero la compañía alcanzó una resolución amistosa con la FTC, como ya se mencionó.

La FTC también resolvió cargos similares con ASUS por la seguridad de sus enrutadores en 2016, cuando la compañía acordó someterse a auditorías de seguridad independientes cada 2 años por los próximos 20 años.