Hasta 29 modelos distintos de router de DrayTek han sido identificados como afectados por una vulnerabilidad crítica de ejecución remota de código no autenticado que, de ser explotada con éxito, podría comprometer completamente el dispositivo y el acceso no autorizado a la red más amplia.

> *«El ataque se puede realizar sin la intención del usuario si la interfaz de administración del dispositivo se ha configurado para estar orientada a Internet. También se puede realizar un ataque con un solo clic desde dentro de la LAN en la configuración predeterminada del dispositivo»,* dijo Philippe Laulheret, investigador de Trellix.

Rastreada como CVE-2022-32548, la vulnerabilidad recibió la calificación de gravedad máxima de 10.0 en el sistema de puntuación CVSS, debido a su capacidad para permitir que un atacante tome el control de los routers completamente.

En esencia, la deficiencia es el resultado de una falla de desbordamiento de búfer en la interfaz de administración web («/cgi-bin/wlogin.cgi»), que puede ser armada por un atacante al proporcionar información especialmente diseñada.

> *«La consecuencia de este ataque es la adquisición del llamado 'DrayOS' que implementa las funcionalidades del router. En los dispositivos que tienen un sistema operativo Linux subyacente (como el Vigor 3910), es posible pasar al sistema operativo subyacente y establecer un punto de apoyo confiable en el dispositivo y la red local»,* dijo Laulheret.

Al parecer, más de 200,000 dispositivos del fabricante taiwanés tienen el servicio vulnerable actualmente expuesto en Internet, y no requerirían la interacción del usuario para ser explotados.

La violación de un dispositivo de red como Vigor 3910 no solo podría dejar una red abierta a acciones maliciosas como el robo de credenciales y propiedad intelectual, actividad de botnet o un ataque de ransomware, sino que también podría causar una condición de denegación de servicio (DoS).

La revelación se produce poco más de un mes después de que surgiera que los routers de ASUS, Cisco, DrayTek y NETGEAR están siendo atacados por un nuevo malware llamado ZuoRAT, que tienen como objetivo las redes de América del Norte y Europa.

Aunque hasta ahora no hay signos de explotación de la vulnerabilidad en la naturaleza, se recomienda aplicar los parches de firmware lo antes posible para protegerse contra posibles amenazas.

> *«Los dispositivos de borde, como el router Vigor3910, viven en el límite entre las redes internas y externas. Como tales, son un objetivo principal para los ciberdelincuentes y los atacantes de amenazas por igual. La violación remota de dispositivos de borde puede llevar a un compromiso total de la red interna de las empresas»,* agregó Laulheret.