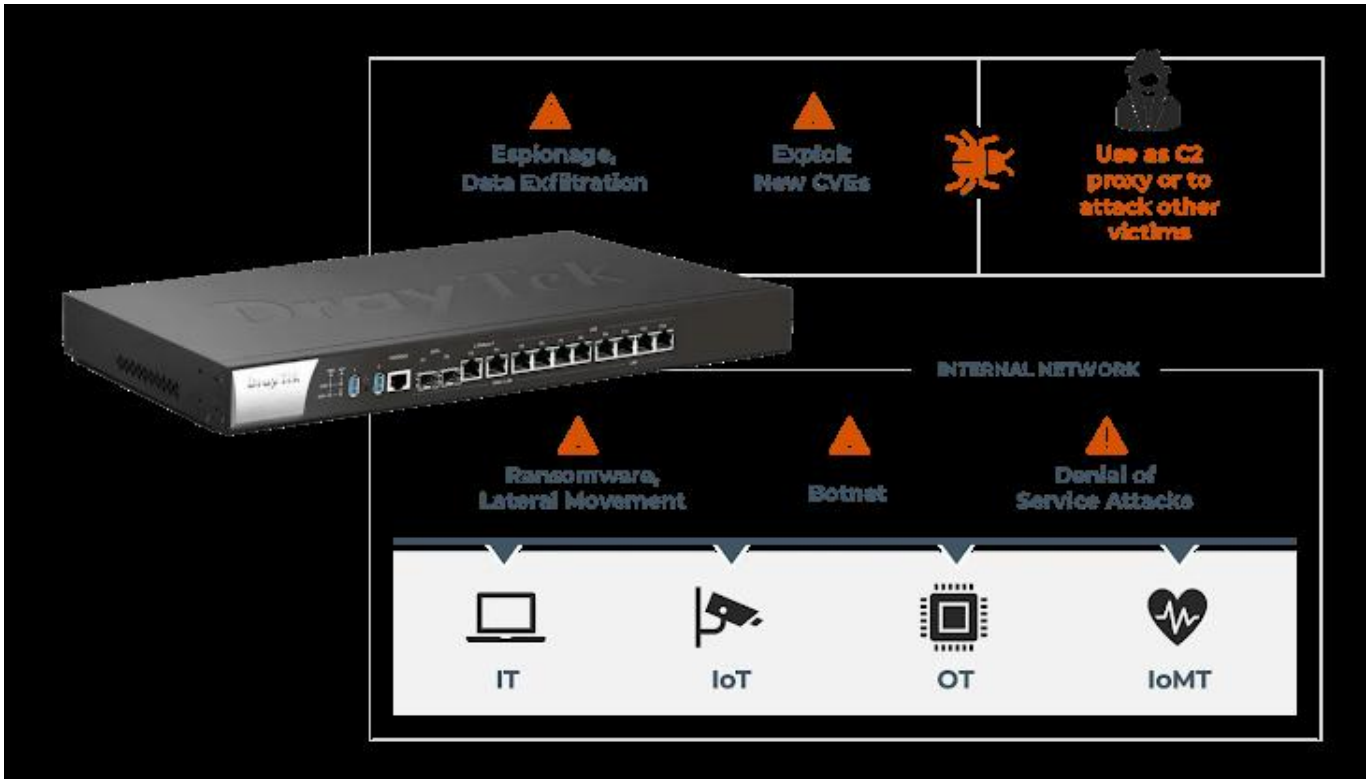
Se han identificado más de una docena de nuevas vulnerabilidades de seguridad en los routers residenciales y empresariales fabricados por DrayTek, que podrían ser aprovechadas por atacantes para tomar el control de los dispositivos afectados.

> *«Estas vulnerabilidades podrían permitir a los atacantes comprometer un router inyectando código malicioso, lo que les daría la capacidad de mantenerse en el dispositivo y usarlo como una puerta de acceso a las redes empresariales»*, señaló Forescout Vedere Labs en un informe técnico.

De las 14 vulnerabilidades descubiertas, dos se consideran críticas, nueve se califican como de alta gravedad y tres son de severidad media. La falla más crítica ha recibido la calificación máxima de CVSS de 10.0.



Esta vulnerabilidad corresponde a un error de desbordamiento de búfer en la función «GetCGI()» de la interfaz web, lo que podría generar una denegación de servicio (DoS) o permitir la ejecución remota de código (RCE) al procesar los parámetros de la cadena de consulta.

Otra vulnerabilidad crítica implica una inyección de comandos en el sistema operativo (OS) en el binario «recvCmd», que se utiliza para la comunicación entre el OS principal y el invitado.

Las otras 12 vulnerabilidades son las siguientes:

- Uso de las mismas credenciales de administrador en todo el sistema, lo que podría permitir la toma de control total del sistema (puntuación CVSS: 7.5).
- Vulnerabilidad de cross-site scripting (XSS) reflejada en la interfaz web (puntuación CVSS: 7.5).
- Vulnerabilidad de XSS almacenada en la interfaz web al configurar un mensaje de bienvenida personalizado después de iniciar sesión (puntuación CVSS: 4.9).
- Vulnerabilidad de XSS almacenada en la interfaz web al establecer un nombre personalizado para el router que se muestra a los usuarios (puntuación CVSS: 4.9).
- Vulnerabilidad de XSS reflejada en la página de inicio de sesión de la interfaz web (puntuación CVSS: 4.9).
- Vulnerabilidades de desbordamiento de búfer en las páginas CGI de la interfaz web «/cgi-bin/v2x00.cgi» y «/cgi-bin/cgiwcg.cgi», que pueden provocar DoS o RCE (puntuación CVSS: 7.2).
- Vulnerabilidades de desbordamiento de búfer en las páginas CGI de la interfaz web que pueden causar DoS o RCE (puntuación CVSS: 7.2).
- Vulnerabilidad de desbordamiento de búfer en la página «/cgi-bin/ipfedr.cgi» de la interfaz web, que puede generar DoS o RCE (puntuación CVSS: 7.2).
- Múltiples vulnerabilidades de desbordamiento de búfer en la interfaz web que pueden ocasionar DoS o RCE (puntuación CVSS: 7.2).
- Vulnerabilidad de desbordamiento de búfer basado en el montón en la función ft_payloads_dns() de la interfaz web, que puede causar DoS (puntuación CVSS: 7.2).

- Vulnerabilidad de escritura fuera de los límites en la interfaz web, que puede derivar en DoS o RCE (puntuación CVSS: 7.2).
- Vulnerabilidad de divulgación de información en el backend del servidor web de la interfaz, que podría permitir a un atacante realizar un ataque de «adversario en el medio» (AitM) (puntuación CVSS: 7.6).

El análisis realizado por Forescout reveló que más de 704,000 routers DrayTek tienen su interfaz web accesible desde internet, lo que los convierte en un objetivo atractivo para los atacantes. La mayor cantidad de instancias expuestas se encuentran en Estados Unidos, seguidas de Vietnam, los Países Bajos, Taiwán y Australia.

Device Model	Fixed versions	EoL?
Vigor1000B, Vigor2962, Vigor3910	4.3.2.8 and 4.4.3.1	**No**
Vigor3912	4.3.6.1	**No**
Vigor165, Vigor166	4.2.7	**No**
Vigor2135, Vigor2763, Vigor2765, Vigor2766	4.4.5.1	**No**
Vigor2865, Vigor2866, Vigor2915	4.4.5.3	**No**
Vigor2620, VigorLTE200	3.9.8.9	Yes
Vigor2133, Vigor2762, Vigor2832	3.9.9	Yes
Vigor2860, Vigor2925	3.9.8	Yes
Vigor2862, Vigor2926	3.9.9.5	Yes
Vigor2952, Vigor3220	3.9.8.2	Yes

Después de una divulgación responsable, DrayTek ha publicado actualizaciones para todas las vulnerabilidades detectadas, incluyendo la más crítica en 11 modelos que ya han llegado al final de su vida útil (EoL).

> *«Para lograr una protección total contra las nuevas vulnerabilidades, es necesario aplicar parches a los dispositivos que utilizan el software afectado. Si su enrutador tiene habilitado el acceso remoto, desactívelo si no es necesario. Utilice una lista de control de acceso (ACL) y autenticación de dos factores (2FA) si es factible»,* afirmó Forescout.

Este avance ocurre mientras agencias de ciberseguridad de Australia, Canadá, Alemania, Japón, Países Bajos, Nueva Zelanda, Corea del Sur, Reino Unido y Estados Unidos han emitido una guía conjunta para organizaciones de infraestructura crítica, con el fin de ayudar a mantener un entorno de tecnología operativa (OT) seguro y protegido.

El documento, titulado *«Principios de ciberseguridad en tecnología operativa»*, detalla seis reglas fundamentales:

1. La seguridad es lo más importante.
2. Conocer el negocio es esencial.
3. Los datos de OT son extremadamente valiosos y deben ser resguardados.
4. Segmentar y aislar OT de todas las demás redes.
5. La cadena de suministro debe ser segura.
6. Las personas son clave para la ciberseguridad en OT.

> *«Filtrar rápidamente las decisiones para identificar aquellas que afectan la seguridad de OT mejorará la capacidad de tomar decisiones sólidas, informadas y completas que favorezcan la seguridad, la protección y la continuidad del negocio al diseñar, implementar y gestionar entornos de OT»*, afirmaron las agencias.