Un equipo de cuatro investigadores de seguridad cibernética daneses, reveló esta semana una falla de seguridad que afecta a los módems de cable que utilizan chips Broadcom.

La vulnerabilidad, nombrada como Cable Haunt, tiene un impacto en aproximadamente 200 millones de módems de cable solo en Europa, según los investigadores.

Esta vulnerabilidad afecta a un componente estándar de los chips Broadcom llamado analizador de espectro. Es un componente de hardware y software que protege el módem de cable de sobretensiones y perturbaciones de señal provenientes del cable coaxial. Los proveedores de servicios de Internet (ISP) suelen utilizar dicho componente para depurar la calidad de la conexión.

En la mayoría de los módems de cable, el acceso a este componente está limitado para las conexiones desde la red interna.

El equipo de investigación dice que el analizador de espectro de chips Broadcom carece de protección contra ataques de reenlace DNS, utiliza credenciales predeterminadas y también contiene un error de programación en su firmware.

Los investigadores aseguran que al engañar a los usuarios para que accedan a una página maliciosa por medio de su navegador, pueden utilizar el navegador para transmitir una vulnerabilidad al componente y ejecutar comandos en el dispositivo. Al aprovechar Cable Haunt, los hackers pueden:

- Cambiar el servidor DNS predeterminado
- Realizar ataques remotos man in the middle
- Código de intercambio en caliente o incluso de todo el firmware
- Cargar o actualizar el firmware silenciosamente
- Deshabilitar la actualización del firmware del ISP
- Cambiar todos los archivos de configuración
- Obtener y establecer valores OID de SNMP
- Cambiar todas las direcciones MAC asociadas

- Cambiar números de serie
- Ser explotado en botnet

Aunque el equipo de investigación estimó que la cantidad de dispositivos vulnerables es de unos 200 millones en toda Europa, se cree que la cantidad total de dispositivos explotables es imposible de cuantificar.

> *«La razón de esto es que la vulnerabilidad se originó en el software de referencia, que aparentemente han sido copiados por diferentes fabricantes de módems de cable al crear su firmware de módem de cable. Esto significa que no hemos podido rastrear la propagación exacta de la vulnerabilidad, y que podría presentarse de formas ligeramente diferentes para muchos fabricantes»,* dijeron los investigadores.

Prueba de concepto disponible

El equipo de investigación publicó esta semana un libro blanco y un sitio web dedicado con información sobre Cable Haunt.

> *«El propósito de este sitio web es informar a tantos usuarios y proveedores afectados como sea posible, a fin de mejorar su capacidad de protegerse».*

La idea principal es que los IPS prueben sus dispositivos y luego publiquen actualizaciones de firmware para parchear el vector de ataque de Cable Haunt. Hasta ahora, cuatro IPS en Escandinavia lanzaron parches (Telia, TDC, Get As y Stofa), pero muchos otros en Europa no lo han hecho, o no son conscientes de la falla.

El equipo de investigación no pudo probar todos los modelos de módem de cable basados en Broadcom que se utilizan actualmente. Aunque confirmaron que algunos módems de cable son vulnerables, muchos modelos de permanecen sin probar.

Los investigadores publicaron un código de prueba de concepto que los ISP y los usuarios expertos en tecnología pueden usar y probar su módem de cable y ver si es vulnerable a un ataque de Cable Haunt.

Algo interesante sobre esta vulnerabilidad es que el ataque es extremadamente complejo para llevarlo a cabo, principalmente porque el componente analizador de espectro vulnerable solo está disponible en la red interna del módem de cable y no está directamente expuesto a Internet.

La explotación de Cable Haunt requiere que un atacante pase por varios aros en un proceso de distintos pasos, lo que hace que este ataque sea altamente improbable para ser utilizado por los operadores de botnets. Sin embargo, el ataque no está fuera del alcance de un atacante determinado que busca comprometer un objetivo de alto valor.