Cisco dijo que no corregirá una vulnerabilidad crítica en los routers para pequeñas empresas debido a que los dispositivos llegaron al final de su vida útil en 2019.

Rastreada como CVE-2021-34730 con puntaje CVSS de 9.8, la vulnerabilidad reside en el servicio Universal Plug-and-Play (UPnP) de los routers, lo que permite que un atacante remoto no autenticado ejecute código arbitrario o haga que un dispositivo afectado se reinicie inesperadamente, lo que resulta en una condición de denegación de servicio (DoS).

La vulnerabilidad, que según la compañía se debe a una validación incorrecta del tráfico UPnP entrante, podría abusarse para enviar una solicitud UPnP especialmente diseñada a un dispositivo afectado, lo que resultaría en la ejecución remota de código como usuario root en el sistema operativo subyacente.

> *«Cisco no ha lanzado y no lanzará actualizaciones de software para abordar la vulnerabilidad. Los routers Cisco Small Business RV110W, RV130, RV130W y RV215W han entrado en el proceso de final de vida útil. Se recomienda a los clientes que migren a los routers Cisco Small Business RV132W, RV160 o RV160W»*, dijo la compañía.

La vulnerabilidad afecta a los siguientes productos:

- Firewall VPN RV110W Wireless-N
- Routers VPN RV130
- Routers VPN multifunción Wireless-N RV130W
- Routers VPN RV215W Wireless-N

En ausencia de un parche, Cisco recomienda a los clientes que deshabiliten UPnP en la interfaz LAN. A Quentin Kaiser de IoT Inspector Research Lab se le atribuyó el crédito por informar sobre la vulnerabilidad.

> *«Con mucha frecuencia, luego de que se reemplaza un sistema o servicio, el sistema o servicio heredado se deja funcionando por si acaso se vuelve a necesitar. El problema radica en el hecho de que, como en el caso de esta vulnerabilidad en Universal Plug-and-Play service: el sistema o servicio heredado generalmente no se mantiene actualizado con actualizaciones o configuraciones de seguridad»*, dijo Dean Ferrando, gerente de ingenieros de sistemas (EMEA) de Tripwire.
>
> *«Esto lo convierte en un excelente objetivo para los malos actores, razón por la que las organizaciones que todavía usan estos viejos enrutadores VPN deben tomar medidas inmediatamente para actualizar sus dispositivos. Esto debe ser parte de un esfuerzo general para fortalecer los sistemas en toda la superficie de ataque, que ayuda a salvaguardar la integridad de los activos digitales y protege contra vulnerabilidades y amenazas de seguridad comunes que pueden aprovecharse como puntos de entrada»,* agregó Ferrando.

CVE-2021-34730 marca la segunda vez que la compañía ha seguido el enfoque de no lanzar correcciones para enrutadores al fin de su vida útil desde inicios del año. A principios de abril, Cisco insistió a los usuarios a actualizar sus routers como contramedida para resolver un error de ejecución de código remoto similar (CVE-2021-1459) que afecta al firewall RV110W VPN y a los routers RV130, RV130W y RV215W para pequeñas empresas.

Además, Cisco también emitió una alerta por una vulnerabilidad crítica de BadAlloc que afecta al sistema operativo en tiempo real (RTOS) BlackBerry QNX que salió a la luz a inicios de esta semana, indicando que la compañía está *«investigando su línea de productos para determinar qué productos y servicios pueden verse afectados por esta vulnerabilidad».*