BOLETÍN DE ALERTA

Boletín Nro.: 2021-37

Fecha de publicación: 13/12/2021

Tema: Vulnerabilidad de ejecución remota de comandos en el firmware del dispositivo TP-Link TL-WR840N v5

Software afectado:

- *Firmware TL-WR840N(EU)_V5_171211 del dispositivo TP-Link TL-WR840N v5*

Descripción:

La vulnerabilidad CVE-2021-41653 con criticidad 9.8 afecta al firmware *TL-WR840N(EU)_V5_171211*, puede ser explotada por un usuario malintencionado que se encuentre autenticado en el dispositivo permitiendo ejecutar comandos de forma remota en el dispositivo con el firmware vulnerable (RCE).

La función *PING del dispositivo* no valida el *input* de IP permitiendo a un atacante que se encuentra autenticado en el dispositivo, pueda crear un *payload* malicioso y ejecutar código remoto en el dispositivo afectado (router).

Se encuentran publicados varias pruebas de conceptos (PoC), caracterizados por ser fácilmente desplegados, por lo que recomendamos actualizar el firmware lo más pronto posible.

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante remoto ejecutar código arbitrario en el sistema.

Detección:

Para comprobar si es probable que su aplicación se vea afectada, debe verificar que la versión del firmware sea inferior a la V5_211109.

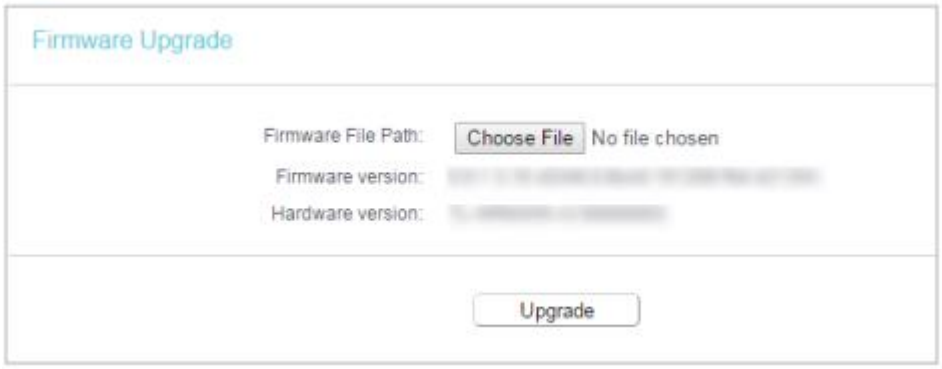
Solución:

Instalar las actualizaciones publicadas por el equipo de TP-LINK previo análisis del impacto que podría provocar en los servicios críticos para el negocio de su organización. En el siguiente enlace puede encontrar el firmware para descargar.

- https://www.tp-link.com/no/support/download/tl-wr840n/v5/#Firmware

Para la actualización del firmware puede seguir las siguientes instrucciones

1. Descargar la última versión del firmware.
2. Ir al sitio http://tplinkwifi.net, ingresar con los datos autenticación del router.
3. Ir a la opción ***System Tools*** > ***Firmware Upgrade***.
4. Seleccionar la opción ***Choose File*** luego seleccionar el archivo del firmware descargado y hacer clic en la opción ***Upgrade***



Información adicional:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41653
- https://nvd.nist.gov/vuln/detail/CVE-2021-41653
- https://k4m1ll0.com/cve-2021-41653.html
- https://vuldb.com/?id.186650
- https://www.incibe-cert.es/en/early-warning/vulnerabilities/cve-2021-41653
- https://www.tp-link.com/no/support/download/tl-wr840n/v5/#Firmware