BOLETÍN DE ALERTA

Boletín Número: 2021-07. **Fecha de Publicación:** 18/08/2021

Tema: Múltiples vulnerabilidades en Realtek SDK afectan a varios fabricantes

Importancia: Crítica.

Descripción:

El Departamento de Ciberseguridad de la DIGETIC/FFAA, informa de la publicación de varias vulnerabilidades en Realtek SDK afectan a varios fabricantes.

Se ha notificado de 4 vulnerabilidades, 2 de severidad crítica y 2 altas, en Realtek SDk que podrían permitir a los atacantes no identificados comprometer completamente el dispositivo de destino y ejecutar código arbitrario con el más alto nivel de privilegio.

Recursos Afectados:

Realtek AP-Router SDK, versiones:

- Realtek SDK, versiones 2.x;
- Realtek "Jungle" SDK, versiones 3.0, 3.1, 3.2, 3.4.x, 3.4T y 3.4T-CT;
- Realtek "Luna" SDK, hasta la versión 1.3.2;
- rtl819x-SDK-v3.2.x Series;
- rtl819x-SDK-v3.4.x Series;
- rtl819x-SDK-v3.4T Series;
- rtl819x-SDK-v3.4T-CT Series;
- rtl819x-eCos-v1.5.x Series.

Detalle

La herramienta MP UDPServer está afectada por múltiples vulnerabilidades de desbordamiento de búfer y una vulnerabilidad de inyección de comandos arbitrarios, debido a que no se puede comprobar suficientemente la legalidad de los comandos recibidos de los clientes. Se ha asignado el identificador CVE-2021-35394 para esta vulnerabilidad **crítica**.

El servidor web HTTP boa (go-ahead ha quedado obsoleto) es vulnerable a múltiples desbordamientos de búfer debido a copias inseguras de algunos parámetros demasiado largos enviados en el formulario. Se ha asignado el identificador CVE-2021-35395 para esta vulnerabilidad crítica.

Solución:

- Realtek SDK 2.x: ya no recibe soporte de Realtek.
- Para Realtek "Jungle" SDK, los parches serán proporcionados por Realtek y necesitan realizar backporting.
- Para Realtek "Luna" SDK, actualizar a la versión 1.3.2a.

Referencias:

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf
https://www.iot-inspector.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/
https://www.iot-inspector.com/blog/realtek-security-vulnerabilities-affect-hardware-manufacturers/