Se ha descubierto una importante vulnerabilidad de seguridad en el *Microchip Advanced Software Framework* (ASF), que podría permitir la ejecución remota de código si se explota con éxito.

Identificada como CVE-2024-7490, esta falla tiene una puntuación de 9.5 en la escala CVSS, donde el máximo es 10.0. Se trata de un desbordamiento de pila en la implementación del servidor tinydhcp de ASF, causado por la falta de validación adecuada de los datos de entrada.

> *«Existe una vulnerabilidad en todos los ejemplos públicos disponibles del código base de ASF que permite que una solicitud DHCP manipulada provoque un desbordamiento de pila, lo que podría dar lugar a la ejecución remota de código»,* señaló el *CERT Coordination Center* (CERT/CC) en un comunicado.

Dado que el software ya no recibe soporte y está basado en código orientado al IoT, CERT/CC ha advertido que es *«probable que esta vulnerabilidad aparezca en muchos sistemas expuestos».*

Este problema afecta a la versión 3.52.0.2574 de ASF y todas las versiones anteriores. Además, la agencia indicó que es probable que varias bifurcaciones del software tinydhcp también sean vulnerables.

Actualmente no hay soluciones ni mitigaciones disponibles para corregir la CVE-2024-7490, salvo reemplazar el servicio tinydhcp por otro que no tenga el mismo defecto.

Este descubrimiento coincide con un informe de *SonicWall Capture Labs*, que reveló una peligrosa vulnerabilidad de «cero clic» en los chipsets Wi-Fi de MediaTek (CVE-2024-20017, CVSS 9.8), que podría permitir la ejecución remota de código sin necesidad de interacción del usuario, debido a un problema de escritura fuera de los límites.

> *«Las versiones afectadas incluyen el SDK de MediaTek en su versión 7.4.0.1 y anteriores, además de OpenWrt 19.07 y 21.02. Esto implica una amplia gama de dispositivos vulnerables, incluyendo enrutadores y teléfonos inteligentes»,* señaló la empresa.
>
> *«La falla es un desbordamiento de búfer que ocurre cuando un valor de longitud, controlado por el atacante, se toma de los datos del paquete sin verificar los límites y se copia en la memoria. Esto provoca una escritura fuera de los límites».*

MediaTek lanzó un parche para esta vulnerabilidad en marzo de 2024, pero la probabilidad de explotación ha aumentado debido a la publicación de un exploit de prueba de concepto (PoC) el 30 de agosto de 2024.