ASUS ha distribuido actualizaciones de su software para corregir un defecto de seguridad grave en sus routers, el cual podría ser aprovechado por individuos malintencionados para sortear los mecanismos de autenticación.

Identificada como CVE-2024-3080, esta vulnerabilidad recibe una calificación CVSS de 9.8, siendo 10.0 la máxima posible.

> *"Algunos modelos específicos de routers de ASUS presentan una vulnerabilidad que permite la omisión de la autenticación, dando lugar a que atacantes remotos sin autenticar puedan acceder al dispositivo",* es lo que se describe sobre el error por parte del Centro de Coordinación/Respuesta a Emergencias Informáticas de Taiwán (TWCERT/CC).

Además, la empresa con sede en Taiwán ha solucionado una falla crítica de desbordamiento de búfer, identificada como CVE-2024-3079 (con una puntuación CVSS de 7.2), que atacantes remotos con privilegios de administrador podrían explotar para ejecutar comandos arbitrarios en el dispositivo.

En un escenario de ataque teórico, un agente dañino podría utilizar CVE-2024-3080 y CVE-2024-3079 en conjunto para crear una secuencia de explotación que les permita evadir la autenticación y correr código malicioso en los dispositivos vulnerables.

Los siguientes productos están afectados por estas debilidades:

- ZenWiFi XT8 versión 3.0.0.4.388_24609 y anteriores (corregido en 3.0.0.4.388_24621)
- ZenWiFi XT8 versión V2 3.0.0.4.388_24609 y anteriores (corregido en 3.0.0.4.388_24621)
- RT-AX88U versión 3.0.0.4.388_24198 y anteriores (corregido en 3.0.0.4.388_24209)
- RT-AX58U versión 3.0.0.4.388_23925 y anteriores (corregido en 3.0.0.4.388_24762)
- RT-AX57 versión 3.0.0.4.386_52294 y anteriores (corregido en 3.0.0.4.386_52303)
- RT-AC86U versión 3.0.0.4.386_51915 y anteriores (corregido en 3.0.0.4.386_51925)

- RT-AC68U versión 3.0.0.4.386_51668 y anteriores (corregido en 3.0.0.4.386_51685)

A principios de enero, ASUS solucionó otra vulnerabilidad crítica identificada como (CVE-2024-3912 , puntuación CVSS: 9.8) que podría permitir a un atacante remoto no autenticado cargar archivos arbitrarios y ejecutar comandos del sistema en el dispositivo.

Se recomienda encarecidamente a los usuarios con routers afectados que actualicen sus dispositivos a la versión más reciente para protegerse contra posibles amenazas.