La compañía taiwanesa ASUS lanzó el lunes actualizaciones de firmware para solucionar, entre otros problemas, nueve fallas de seguridad que afectan a una amplia variedad de modelos de routers.

De las nueve vulnerabilidades de seguridad, dos son consideradas críticas y seis tienen un nivel alto de gravedad. Actualmente, se está analizando una vulnerabilidad pendiente.

Los productos afectados incluyen GT6, GT-AXE16000, GT-AX11000 PRO, GT-AXE11000, GT-AX6000, GT-AX11000, GS-AX5400, GS-AX3000, XT9, XT8, XT8 V2, RT-AX86U PRO, RT-AX86U, RT-AX86S, RT-AX82U, RT-AX58U, RT-AX3000, TUF-AX6000 y TUF-AX5400.

Destacan en la lista de correcciones las vulnerabilidades CVE-2018-1160 y CVE-2022-26376, ambas con una puntuación de 9.8 sobre un máximo de 10 en el sistema de puntuación CVSS.

CVE-2018-1160 se refiere a un error de escritura fuera de límites en versiones anteriores a 3.1.12 de Netatalk que lleva casi cinco años existiendo y que podría permitir que un atacante no autenticado remoto logre ejecutar código arbitrario.

CVE-2022-26376 ha sido descrita como una vulnerabilidad de corrupción de memoria en el firmware de Asuswrt que podría activarse mediante una solicitud HTTP especialmente creada.

Las otras siete vulnerabilidades son las siguientes:

- CVE-2022-35401 (puntuación CVSS: 8.1) – Una vulnerabilidad de bypass de autenticación que podría permitir que un atacante envíe solicitudes HTTP maliciosas para obtener acceso administrativo completo al dispositivo.
- CVE-2022-38105 (puntuación CVSS: 7.5) – Una vulnerabilidad de divulgación de información que podría ser explotada para acceder a información confidencial mediante el envío de paquetes de red especialmente diseñados.
- CVE-2022-38393 (puntuación CVSS: 7.5) – Una vulnerabilidad de denegación de servicio (DoS) que podría activarse mediante el envío de un paquete de red

especialmente diseñado.

- CVE-2022-46871 (puntuación CVSS: 8.8) – El uso de una biblioteca libusrsctp desactualizada que podría exponer los dispositivos afectados a otros ataques.
- CVE-2023-28702 (puntuación CVSS: 8.8) – Una falla de inyección de comandos que podría ser aprovechada por un atacante local para ejecutar comandos de sistema arbitrarios, interrumpir el sistema o finalizar el servicio.
- CVE-2023-28703 (puntuación CVSS: 7.2) – Una vulnerabilidad de desbordamiento de búfer basada en la pila que podría ser explotada por un atacante con privilegios de administrador para ejecutar comandos de sistema arbitrarios, interrumpir el sistema o finalizar el servicio.
- CVE-2023-31195 (puntuación CVSS: N/A) Una vulnerabilidad de adversario-en-medio (AitM) que podría llevar al secuestro de la sesión de un usuario.

ASUS recomienda a los usuarios aplicar las últimas actualizaciones lo antes posible para mitigar los riesgos de seguridad. Como solución temporal, sugiere desactivar los servicios accesibles desde el lado de la WAN para evitar posibles intrusiones no deseadas.

«Estos servicios incluyen acceso remoto desde la WAN, reenvío de puertos, DDNS, servidor VPN, DMZ y activación de puertos», dijo la compañía, instando a los clientes a realizar auditorías periódicas de sus equipos, así como a configurar contraseñas separadas para la red inalámbrica y la página de administración del router.