Se han revelado vulnerabilidades de seguridad en los routers Netcomm y TP-Link, algunos de los cuales podrían armarse para lograr la ejecución remota de código.

Las vulnerabilidades, rastreadas como CVE-2022-4873 y CVE-2022-4874, se refieren a un caso de desbordamiento de búfer basado en pila y omisión de autenticación y afectan a los modelos de enrutador Netcomm NF20MESH, NF20 y NL1902 que ejecutan versiones de firmware anteriores a R6B035.

> *«Las dos vulnerabilidades, cuando se encadenan juntas, permiten que un atacante remoto no autenticado ejecute código arbitrario»,* dijo el Centro de Coordinación CERT (CERT/CC) en un aviso.

> *«El atacante primero puede obtener acceso no autorizado a los dispositivos afectados y luego usar esos puntos de entrada para obtener acceso a otras redes o comprometer la disponibilidad, integridad o confidencialidad de los datos que se transmiten desde la red interna».*

Al investigador de seguridad Brendan Scarvell se le atribuye el descubrimiento y el informe de los problemas en octubre de 2022.

En un desarrollo relacionado, CERT/CC también detalló dos vulnerabilidades de seguridad sin parchear que afectan a los routers TP-Link WR710N-V1-151022 y Archer-C5-V2-160201, que podrían conducir a la divulgación de información (CVE-2022-4499) y ejecución remota de código (CVE-2022-4498).

CVE-2022-4499 también es un ataque de canal lateral dirigido a una función usada para validar las credenciales ingresadas. *«Al medir el tiempo de respuesta del proceso vulnerable, cada byte de las cadenas de nombre de usuario y contraseña puede ser más fácil de adivinar»,* dijo CERT/CC.

El investigador de Microsoft, James Hull, fue reconocido por revelar los dos errores.