En un último estudio titulado «*SOHOpelessly Broken 2.0*«, los Evaluadores de Seguridad Independientes (ISE), descubrieron un total de 125 vulnerabilidades de seguridad diferentes en 13 enrutadores de pequeñas oficinas (SOHO) y dispositivos de almacenamiento conectado a la red (NAS), que probablemente afecten a millones de personas.

> *«Hoy mostramos que los controles de seguridad establecidos por los fabricantes de dispositivos son insuficientes contra los ataques llevados a cabo por adversarios remotos. Este proyecto de investigación tuvo como objetivo descubrir y aprovechar nuevas técnicas para eludir estos nuevos controles de seguridad en dispositivos integrados»,* afirmaron los investigadores.

Routers afectados

Los routers SOHO y dispositivos NAS probados por los investigadores son de los siguientes fabricantes:

- Buffalo
- Synology
- TerraMaster
- Zyxel
- Drobo
- ASUS and its subsidiary Asustor
- Seagate
- QNAP
- Lenovo
- Netgear
- Xiaomi
- Zioncom (TOTOLINK)

Según los investigadores de seguridad, los 13 dispositivos ampliamente utilizados que se probaron, tenían al menos una vulnerabilidad de aplicación web que podría permitir que un

atacante remoto obtuviera acceso de shell remoto o acceso al panel administrativo del dispositivo afectado.

Estas vulnerabilidades varían desde secuencias de comandos entre sitios (XSS), falsificación de solicitudes entre sitios (CSRF), desbordamiento de búfer, inyección de comandos del sistema operativo (OS CMDi), omisión de autenticación, inyección SQL (SQLi) y vulnerabilidades transversales de la ruta de carga de archivos.

Control total sobre los dispositivos sin autenticación

Los investigadores dijeron que obtuvieron con éxito las capas de raíz en 12 de los dispositivos, lo que les permitió tener un control completo sobre los dispositivos afectados, 6 de los cuales contenían fallas que permitirían a los atacantes obtener el control total de un dispositivo de forma remota y sin autenticación.

Estos routers comerciales y domésticos afectados son: Asustor AS-602T, Buffalo TeraStation TS5600D1206, TerraMaster F2-420, Drobo 5N2, Netgear Nighthawk R9000 y TOTOLINK A3002RU.

Desde SOHOpelessly Broken 1.0, los investigadores afirmaron que encontraron algunos dispositivos IoT más nuevos que implementan algunos mecanismos de seguridad útiles, como la aleatorización del diseño del espacio de direcciones (ASLR), funcionalidades que dificultan la ingeniería inversa y mecanismos de verificación de integridad para solicitudes HTTP.

Sin embargo, algunas cosas no han cambiado desde SOHOpelessly Broken 1.0, como muchos dispositivos IoT aún carecen de funciones básicas de protección de aplicaciones web, como tokens anti-CSRF y encabezados de seguridad del navegador, que pueden mejorar en gran medida la postura de seguridad de las aplicaciones web y los sistemas subyacentes con los que interactúan.

Los investigadores del ISE informaron responsablemente de todas las vulnerabilidades que

descubrieron a los fabricantes de dispositivos afectados, la mayoría de los cuales respondieron rápidamente y tomaron medidas de seguridad para mitigar estas vulnerabilidades, que ya recibieron sus ID CVE.

Sin embargo, algunos fabricantes de dispositivos, incluyendo Drobo, Buffalo Americas y Ziocom Holdings, no respondieron a los hallazgos de los investigadores.