Se ha descubierto un conjunto de 38 vulnerabilidades de seguridad en dispositivos inalámbricos de Internet Industrial de las Cosas (IIoT) de cuatro proveedores distintos, que podrían representar una superficie de ataque significativa para los actores de amenazas que buscan explotar los entornos de tecnología operativa (OT).

> *«Los actores de amenazas pueden explotar las vulnerabilidades en los dispositivos inalámbricos IIoT para obtener acceso inicial a las redes OT internas. Pueden usar estas vulnerabilidades para eludir las capas de seguridad e infiltrarse en las redes objetivo, poniendo en riesgo la infraestructura crítica o interrumpiendo la fabricación»*, dijo la compañía de seguridad cibernética Otorio.

Las vulnerabilidades ofrecen un punto de entrada remoto para el ataque, lo que permite que los atacantes no autenticados se afiancen y después lo usen como palanca para propagarse a otros hosts, causando daños significativos.

Algunas de las vulnerabilidades identificadas podrían encadenarse para dar a un atacante acceso directo a miles de redes OT internas por medio de Internet, dijo el investigador de seguridad Roni Gavrilov.

De las 38 vulnerabilidades, tres afectan al servidor de acceso remoto (RAS) de ETIC Telecom (CVE-2022-3703, CVE-2022-41607 y CVE-2022-40981) y podrían abusarse para tomar el control completo de los dispositivos susceptibles.

Otras cinco vulnerabilidades se refieren a InHand Networks InRouter 302 e InRouter 615, que de ser explotadas, podrían resultar en la inyección de comandos, la divulgación de información y la ejecución de código.

Específicamente, implica aprovechar los problemas en la plataforma en la nube *«Administrador de dispositivos»,* que permite a los operadores realizar acciones remotas como cambios de configuración y actualizaciones de firmware, con el fin de comprometer todos los dispositivos InRouter administrados en la nube con privilegios de root.

También se identificaron dos vulnerabilidades en Sierra Wireless AirLink Router (CVE-2022-46649 y CVE-2022-46650), que podrían permitir la pérdida de información confidencial y la ejecución remota de código. Los defectos restantes aún siguen bajo divulgación responsable.

Los hallazgos subrayan cómo las redes OT podrían ponerse en riesgo al hacer que los dispositivos IIoT sean directamente accesibles en Internet, creando efectivamente un *«punto único de falla»* que puede eludir todas las protecciones de seguridad.

De forma alterna, los atacantes locales pueden ingresar a puntos de acceso WiFi industriales y puertas de enlace celulares al apuntar a canales celulares o WiFi en el sitio, lo que lleva a escenarios de adversario en el medio (AitM) con un impacto potencial adverso.

Los ataques pueden ir desde esquemas de encriptación débiles dirigidos a ataques de coexistencia dirigidos a chips combinados que se usan ampliamente en dispositivos electrónicos.

Para poder lograr esto, los hackers pueden utilizar plataformas como WiGLE, una base de datos de diferentes puntos de acceso inalámbricos en todo el mundo, para identificar entornos industriales de alto valor, ubicarlos físicamente y explotar los puntos de acceso desde la proximidad, dijo Otorio.

Como contramedidas, se recomienda deshabilitar los esquemas de encriptación inseguros, ocultar los nombres de las redes WiFi, deshabilitar los servicios de administración de la nube no utilizados y tomar medidas para evitar que los dispositivos sean de acceso público.

> *«La baja complejidad del exploit, combinada con el amplio impacto potencial, hace que los dispositivos IIoT inalámbricos y sus plataformas de administración basadas en la nube sean un objetivo atractivo para los atacantes que buscan violar los entornos industriales»,* dijo la compañía.

El desarrollo también se produce cuando Otorio reveló detalles de dos vulnerabilidades de alta gravedad en Siemens Automation License Manager (CVE-2022-43513 y CVE-2022-43514), que podrían combinarse para obtener ejecución remota de código y escalamiento de privilegios. Siemens corrigió los errores en enero de 2023.