Se revelaron varias vulnerabilidades de seguridad en las plataformas de administración de la nube asociadas con tres proveedores de routers celulares industriales, que podrían exponer las redes de tecnología operativo (OT) a ataques externos.

Los hallazgos fueron presentados por la compañía israelí de seguridad cibernética industrial OTORIO en la conferencia Black Hat Asia 2023 la semana pasada.

Las 11 vulnerabilidades permiten *«la ejecución remota de código y el control total sobre cientos de miles de dispositivos y redes OT, en algunos casos, incluso aquellos que no están configurados activamente para usar la nube».*

Específicamente, las vulnerabilidades residen en las soluciones de administración basadas en la nube que ofrecen Sierra Wireless, Teltonika Networks y InHand Networks para administrar y operar dispositivos remotamente.

La explotación exitosa de las vulnerabilidades podría plantear graves riesgos para los entornos industriales, lo que permitiría a los adversarios eludir las capas de seguridad, filtrar información confidencial y lograr la ejecución remota del código en las redes internas.

Peor todavía, los problemas podrían armarse para obtener acceso no autorizado a dispositivos en la red y realizar operaciones maliciosas, como el apagado con permisos elevados.

Esto, a su vez, es posible gracias a tres vectores de ataque distintos que podrían explotarse para comprometer y apoderarse de dispositivos IIOT administrados en la nube por medio de sus plataformas de administración basadas en la nube:

- Mecanismos débiles de registro de activos (Sierra Wireless): Un atacante podría buscar dispositivos no registrados que estén conectados a la nube, obtener sus números de

serie aprovechando la herramienta AirVantage Online Warranty Checker, registrarlos en una cuenta bajo su control y ejecutar comandos arbitrarios.
- Vulnerabilidades en las configuraciones de seguridad (InHand Networks): Un usuario no autorizado podría aprovechar CVE-2023-22601, CVE-2023-22600 y CVE-2023-22598, una vulnerabilidad de inyección de comandos para obtener la ejecución remota de código con privilegios de raíz, emitir comandos de reinicio y enviar actualizaciones de firmware.
- API e interfaces externas (Teltonika Networks): Un hacker podría abusar de múltiples problemas identificados en el sistema de administración remota (RMS) para *«exponer información confidencial del dispositivo y credenciales del dispositivo, permitir la ejecución remota de código, exponer dispositivos conectados administrados en la red y permitir la suplantación de dispositivos legítimos»*.

Las seis vulnerabilidades que afectan a Teltonika Networks (CVE-2023-32346, CVE-2023-32347, CVE-2023-32348, CVE-2023-2586, CVE-2023-2587 y CVE-2023-2588) se descubrieron luego de una *«completa investigación»* realizada en colaboración con Claroty.

> *«Un atacante que explote con éxito estos enrutadores industriales y dispositivos IoT puede causar una serie de impactos en dispositivos y redes comprometidos, incluyendo el monitoreo del tráfico de red y el robo de datos confidenciales, el secuestro de conexiones a Internet y el acceso a servidores internos»*, dijeron las compañías.

OTORIO dijo que los dispositivos administrados en la nube representan un riesgo «enorme» para la cadena de suministro y que el compromiso de un solo proveedor puede actuar como una puerta trasera para acceder a varias redes OT de una sola vez.

El desarrollo se produce poco más después de tres meses de que la compañía de seguridad cibernética revelara 38 fallas de seguridad en los dispositivos inalámbricos industriales de Internet de las cosas (IIoT) que podrían proporcionar a los atacantes una ruta directa a las redes OT internas y poner en riesgo la infraestructura crítica.

> *«A medida que la implementación de dispositivos IIoT se vuelve más popular, es importante tener en cuenta que sus plataformas de administración en la nube pueden ser atacadas por hackers. La explotación de una única plataforma de proveedor de IIoT podría actuar como un 'punto de pivote' para los atacantes, accediendo a miles de entornos a la vez»*, dijo el investigador de seguridad Roni Gavrilov.