Se han revelado varias vulnerabilidades de seguridad de alta gravedad en los enrutadores de borde ER2000 de ConnectedIO y en la plataforma de gestión basada en la nube, que podrían ser aprovechadas por actores maliciosos para ejecutar código perjudicial y acceder a información confidencial.

> *«Un atacante podría haber utilizado estas debilidades para comprometer completamente la infraestructura en la nube, ejecutar código de forma remota y filtrar toda la información de clientes y dispositivos»*, mencionó Noam Moshe de Claroty en un análisis publicado recientemente.

Las vulnerabilidades en los enrutadores 3G/4G podrían poner en riesgo miles de redes internas, lo que permitiría a los actores maliciosos tomar el control, interceptar el tráfico e incluso infiltrarse en objetos de Internet de las Cosas Extendido (XIoT).

Las deficiencias que afectan a las versiones anteriores a v2.1.0 de la plataforma ConnectedIO, principalmente en el enrutador de borde 4G ER2000 y los servicios en la nube, podrían ser conectadas, lo que permitiría a los atacantes ejecutar código arbitrario en los dispositivos basados en la nube sin la necesidad de acceder directamente a ellos.

También se han descubierto fallos en el protocolo de comunicación (es decir, MQTT) utilizado entre los dispositivos y la nube, incluyendo el uso de credenciales de autenticación codificadas en el firmware, que podrían ser empleadas para registrar un dispositivo falso y acceder a mensajes MQTT que contienen identificadores de dispositivos, configuraciones de Wi-Fi, SSID y contraseñas de routers.

Una consecuencia de estas vulnerabilidades es que un actor malicioso no solo podría hacerse pasar por cualquier dispositivo de su elección utilizando los números IMEI filtrados, sino también forzarlos a ejecutar comandos arbitrarios publicados a través de mensajes MQTT especialmente diseñados.

Esto es posible mediante un comando bash con el código de operación *«1116»,* que ejecuta

un comando remoto *«tal cual»*.

> *«Este comando, que no requiere ninguna otra forma de autenticación que la capacidad de escribirlo en el tema correcto, nos permite ejecutar comandos arbitrarios en todos los dispositivos»,* explicó Moshe.

> *«No valida que el remitente de los comandos sea realmente un emisor autorizado. Utilizando este código de operación de comando, pudimos generar una carga útil que resultará en la ejecución de código cada vez que se envíe a un dispositivo».*

Estos problemas se han identificado con los siguientes códigos CVE:

- CVE-2023-33375 (puntuación CVSS: 8.6) – Una vulnerabilidad de desbordamiento de búfer basada en la pila en su protocolo de comunicación, lo que permite que los atacantes tomen el control de los dispositivos.
- CVE-2023-33376 (puntuación CVSS: 8.6) – Una vulnerabilidad de inyección de argumentos en su mensaje de comando de tablas IP en su protocolo de comunicación, permitiendo a los atacantes ejecutar comandos arbitrarios del sistema operativo en los dispositivos.
- CVE-2023-33377 (puntuación CVSS: 8.6) – Una vulnerabilidad de inyección de comandos del sistema operativo en el comando de configuración de firewall en parte de su protocolo de comunicación, permitiendo a los atacantes ejecutar comandos arbitrarios del sistema operativo en los dispositivos.
- CVE-2023-33378 (puntuación CVSS: 8.6) – Una vulnerabilidad de inyección de argumentos en su mensaje de comando AT en su protocolo de comunicación, permitiendo a los atacantes ejecutar comandos arbitrarios del sistema operativo en los dispositivos.

> *«Estas vulnerabilidades, si se explotan, podrían representar un riesgo grave para miles de empresas en todo el mundo, permitiendo a los atacantes interrumpir las operaciones comerciales y la producción de las empresas, además de proporcionar acceso a las redes internas de las empresas»,* comentó Moshe.

Este descubrimiento se produce al mismo tiempo que la empresa también ha revelado una serie de fallos en dispositivos de almacenamiento en red (NAS) de Synology y Western Digital que podrían ser utilizados para suplantar y controlar estos dispositivos, así como para robar datos almacenados y redirigir a los usuarios hacia un dispositivo controlado por un atacante.

También se suma al descubrimiento de tres vulnerabilidades no corregidas que afectan al modelo de bastidor Bently Nevada 3500 de Baker Hughes, las cuales podrían ser utilizadas para evitar el proceso de autenticación y obtener acceso completo al dispositivo y a sus configuraciones internas.

> *«En el escenario más grave, estas fallas podrían permitir que un atacante comprometa completamente el dispositivo y modifique su configuración interna, lo que podría llevar a mediciones incorrectas de las máquinas monitoreadas o a ataques de denegación de servicio»*, afirmó Nozomi Networks.