Investigadores en ciberseguridad han revelado 46 nuevas vulnerabilidades en productos de tres fabricantes de inversores solares: Sungrow, Growatt y SMA. Estas fallas podrían ser aprovechadas por atacantes para tomar el control de los dispositivos o ejecutar código de forma remota, lo que representa un riesgo significativo para las redes eléctricas.

Forescout Vedere Labs ha agrupado estas vulnerabilidades bajo el nombre en clave SUN:DOWN.

> *«Las nuevas vulnerabilidades pueden ser explotadas para ejecutar comandos arbitrarios en dispositivos o en la nube del proveedor, tomar el control de cuentas, obtener acceso a la infraestructura del fabricante o incluso apoderarse de los dispositivos de los propietarios de los inversores»*, explicó la compañía en un informe.

Entre las fallas de seguridad más destacadas se encuentran:

- Los atacantes pueden subir archivos .aspx que serán ejecutados por el servidor web de SMA (*sunnyportal[.]com*), lo que permite la ejecución remota de código.
- Actores no autenticados pueden realizar una enumeración de nombres de usuario a través del endpoint «server.growatt.com/userCenter.do».
- Se puede obtener la lista de plantas solares y dispositivos asociados a otros usuarios mediante el endpoint «server-api.growatt.com/newTwoEicAPI.do», lo que facilita la toma de control de los dispositivos.
- Un atacante no autenticado puede obtener el número de serie de un medidor inteligente utilizando un nombre de usuario válido a través del endpoint «server-api.growatt.com/newPlantAPI.do», lo que podría llevar al secuestro de cuentas.
- Es posible acceder a información sobre cargadores de vehículos eléctricos (EV), consumo energético y otros datos sensibles a través del endpoint «evcharge.growatt.com/ocpp». Además, un atacante podría reconfigurar estos cargadores de forma remota, lo que podría ocasionar daños físicos.
- La aplicación de Android de Sungrow utiliza una clave AES insegura para cifrar datos

del cliente, lo que permitiría a un atacante interceptar y descifrar las comunicaciones entre la app móvil e iSolarCloud.
- La aplicación de Android de Sungrow ignora explícitamente los errores de certificado, haciéndola vulnerable a ataques de *adversary-in-the-middle* (AitM).
- La interfaz web WiNet WebUI de Sungrow contiene una contraseña predefinida que permite descifrar todas las actualizaciones de firmware.
- Existen múltiples vulnerabilidades en la gestión de mensajes MQTT en los dispositivos de Sungrow, lo que podría provocar la ejecución remota de código o condiciones de denegación de servicio (*DoS*).

Forescout advirtió que:

> *«Un atacante que logre comprometer una gran cantidad de inversores Sungrow, Growatt y SMA utilizando estas vulnerabilidades recién descubiertas podría controlar suficiente energía como para desestabilizar estas redes eléctricas y otras de gran escala».*

En un posible ataque contra los inversores Growatt, un ciberdelincuente podría explotar una API expuesta para adivinar los nombres de usuario reales de las cuentas, secuestrarlas restableciendo sus contraseñas al valor predeterminado (*123456*) y continuar con la explotación de los dispositivos.

El problema se agrava aún más si estos inversores comprometidos son utilizados como una botnet para amplificar el ataque, lo que podría ocasionar interrupciones en la red eléctrica e incluso apagones. No obstante, los fabricantes ya han corregido estas vulnerabilidades tras ser notificadas de manera responsable.

Forescout agregó:

> *«Dado que los atacantes pueden controlar flotas completas de dispositivos con*

> *impacto en la producción de energía, pueden modificar su configuración para inyectar más o menos energía a la red en momentos específicos»,* advirtiendo que estas vulnerabilidades exponen las redes eléctricas a ataques de ransomware ciberfísico.

Según Daniel dos Santos, director de investigación en Forescout Vedere Labs, mitigar estos riesgos requiere la implementación de estrictos requisitos de seguridad al adquirir equipos solares, evaluaciones regulares de riesgos y una visibilidad total de estos dispositivos dentro de la red.

Otras vulnerabilidades en dispositivos industriales

Esta revelación ocurre en paralelo a la identificación de fallas críticas en cámaras de monitoreo de líneas de producción fabricadas por la empresa japonesa Inaba Denki Sangyo. Estas vulnerabilidades podrían permitir a un atacante realizar vigilancia remota y evitar la grabación de interrupciones en la producción.

A pesar de que estos fallos aún no han sido corregidos, el fabricante ha recomendado restringir el acceso a internet y asegurarse de que estos dispositivos sean instalados en áreas seguras, accesibles solo para personal autorizado.

La empresa de seguridad Nozomi Networks advirtió:

> *«Estas fallas permiten diversos ataques, incluyendo la posibilidad de que un atacante no autenticado acceda de forma remota y secreta a transmisiones en vivo para vigilancia o interrumpa la grabación de fallos en la línea de producción, impidiendo la captura de momentos críticos».*

En los últimos meses, también se han identificado múltiples vulnerabilidades en dispositivos industriales como el GE Vernova N60 Network Relay, el Zettler 130.8005 Industrial Gateway,

y el Wago 750-8216/025-001 Programmable Logic Controller (PLC), los cuales podrían ser utilizados por atacantes para obtener control total de los sistemas afectados.