Investigadores de seguridad cibernética elaboraron una técnica de ataque novedosa que arma los controladores lógicos programables (PLC) para ganar un punto de apoyo inicial en las estaciones de trabajo de ingeniería, y posteriormente, invadir las redes de tecnología operativa (OT).

Denominado como «Evil PLC» por parte de la compañía de seguridad industrial Claroty, el ataque afecta al software de estación de trabajo de ingeniería de Rockwell Automation, Schneider Electric, GE, B&R, Xinje, OVARRO y Emerson.

Los controladores lógicos programables son componentes cruciales de dispositivos industriales, que controlan los procesos de fabricación en sectores de infraestructura crítica. Los PLC, además de realizar tareas de automatización, también están configurados para iniciar y detener procesos y generar alarmas.

Debido a esto, no sorprende que el acceso arraigado proporcionado por los PLC haya convertido a las máquinas en el foco de ataques sofisticados durante más de diez años, desde Stuxnet hasta PIPEDREAM (también conocido como INCONTROLLER), con el objetivo de causar interrupciones físicas.

> *«Estas aplicaciones de estaciones de trabajo suelen ser un puente entre las redes de tecnología operativa y las redes corporativas. Un atacante que es capaz de comprometer y explotar vulnerabilidades en una estación de trabajo de ingeniería podría pasar fácilmente a la red interna, moverse lateralmente entre sistemas y obtener más acceso a otros PLC y sistemas sensibles»*, dijo Claroty.

Con el ataque Evil PLC, el controlador actúa como un medio para un fin, lo que permite que el atacante acceda a una estación de trabajo, acceda a todos los demás PLC en la red e incluso, altere la lógica del controlador.

Según los investigadores, la idea es *«usar el PLC como un punto de pivote para atacar a los ingenieros que lo programan y lo diagnostican y obtener un acceso más profundo a la red*

OT».

Toda la secuencia se desarrolla de la siguiente forma: un adversario oportunista induce deliberadamente un mal funcionamiento en un PLC expuesto a Internet, una acción que incita a un ingeniero desprevenido a conectarse al PLC infectado utilizando el software de la estación de trabajo de ingeniería como herramienta de solución de problemas.

En la siguiente fase, el atacante aprovecha las vulnerabilidades previamente no descubiertas identificadas en las plataformas para ejecutar código malicioso en la estación de trabajo cuando el ingeniero realiza una operación de carga para recuperar una copia funcional de la lógica del PLC existente.

«El hecho de que el PLC almacene tipos adicionales de datos que usa el software de ingeniería y no el propio PLC» crea un escenario en el que los datos no utilizados almacenados en el PLC pueden modificarse para manipular el software de ingeniería.

> *«En la mayoría de los casos, las vulnerabilidades existen porque el software confiaba plenamente en los datos provenientes del PLC sin realizar controles de seguridad exhaustivos»,* dijeron los investigadores.

En un escenario de ataque teórico alternativo, el método Evil PLC también se puede usar como trampas para atraer a los hackers para que se conecten a un PLC señuelo, lo que lleva a un compromiso de la máquina del atacante.

Claroty también mencionó la ausencia de protecciones de seguridad en los dispositivos del sistema de control industrial (ICS) orientado al público, lo que facilita que los atacantes alteren su lógica por medio de procedimientos de descarga no autorizados.

Para mitigar dichos ataques, se recomienda limitar el acceso físico y de red a los PLC a los ingenieros y operadores autorizados, hacer cumplir los mecanismos de autenticación para validar la estación de ingeniería, monitorear el tráfico de la red OT en busca de actividad anómala y aplicar parches de forma oportuna.