Se revelaron dos nuevas vulnerabilidades de seguridad en los controladores lógicos programables (PLC) y el software de estación de trabajo de ingeniería de Rockwell Automation, que un atacante podría explotar para inyectar código malicioso en los sistemas afectados y modificar sigilosamente los procesos de automatización.

Las fallas tienen el potencial de interrumpir las operaciones industriales y causar daños físicos a las fábricas de forma similar a los ataques de Stuxnet y Rogue7, dijo la compañía de seguridad de tecnología operativa Claroty.

> *«La lógica programable y las variables predefinidas impulsan estos procesos, y los cambios en cualquiera alterarán el funcionamiento normal del PLC y el proceso que administra»,* dijo Sharon Brizinov, de Claroty.

En la siguiente lista se detallan las vulnerabilidades:

- CVE-2022-1161 (puntaje CVSS: 10.0): Una vulnerabilidad explotable de forma remota que permite a un atacante escribir código de programa «textual» legible por el usuario en una ubicación de memoria separada del código compilado ejecutado (también conocido como código de bytes). El problema reside en el firmware del PLC que se ejecuta en los sistemas de control ControlLogix, CompactLogix y GuardLogix de Rockwell.
- CVE-2022-1159 (puntaje CVSS: 7.7): Un atacante con acceso administrativo a una estación de trabajo que ejecuta la aplicación Studio 5000 Logix Designer puede interceptar el proceso de compilación e inyectar código en el programa del usuario sin el conocimiento del usuario.

La explotación exitosa de las vulnerabilidades podría permitir que un atacante modifique los programas de usuario y descargue código malicioso al controlador, alterando de forma efectiva el funcionamiento normal del PLC y permitiendo que se envíen comandos no autorizados a los dispositivos físicos controlados por el sistema industrial.

> *«El resultado final de explotar ambas vulnerabilidades es el mismo: el ingeniero cree que se está ejecutando un código benigno en el PLC; mientras tanto, se está ejecutando un código completamente diferente y potencialmente malicioso en el PLC»*, explicó Brizinov.

La gravedad de las vulnerabilidades también provocó un aviso de la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), que describe los pasos de mitigación que los usuarios del hardware y software afectados pueden tomar para una *«estrategia integral de defensa en profundidad».*