Una vulnerabilidad de seguridad de alta severidad ha sido identificada en los dispositivos Rockwell Automation ControlLogix 1756, que podría ser utilizada para ejecutar comandos de programación y configuración del protocolo industrial común (CIP).

Esta vulnerabilidad, que está identificada con el CVE CVE-2024-6242, tiene una puntuación de 8.4 en la escala CVSS v3.1.

> *«Se ha encontrado una vulnerabilidad en los productos afectados que permite a un atacante eludir la función de Ranura Confiable en un controlador ControlLogix»*, señaló la Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) en un aviso.
>
> *«Si se explota en cualquier módulo afectado dentro de un chasis 1756, un atacante podría potencialmente ejecutar comandos CIP que alteran proyectos de usuario y/o la configuración del dispositivo en un controlador Logix dentro del chasis.»*

La empresa de seguridad en tecnología operativa Claroty, que descubrió e informó sobre la vulnerabilidad, indicó que desarrolló una técnica que permitió eludir la función de ranura confiable y enviar comandos maliciosos a la CPU del controlador lógico programable (PLC).

La función de ranura confiable *«aplica políticas de seguridad y permite al controlador rechazar comunicaciones a través de rutas no confiables en el chasis local«*, explicó la investigadora de seguridad Sharon Brizinov.

> *«La vulnerabilidad que encontramos, antes de ser corregida, permitía a un atacante moverse entre ranuras de la placa de respaldo local dentro de un chasis 1756 usando enrutamiento CIP, cruzando el límite de seguridad destinado a proteger la CPU de tarjetas no confiables.»*

Aunque para un ataque exitoso se requiere acceso a la red del dispositivo, un atacante podría aprovechar la falla para enviar comandos elevados, incluyendo la carga de lógica arbitraria en la CPU del PLC, incluso si el atacante está detrás de una tarjeta de red no confiable.

Después de una divulgación responsable, el problema ha sido solucionado en las siguientes versiones:

- ControlLogix 5580 (1756-L8z) – Actualizar a las versiones V32.016, V33.015, V34.014, V35.011 y posteriores.
- GuardLogix 5580 (1756-L8zS) – Actualizar a las versiones V32.016, V33.015, V34.014, V35.011 y posteriores.
- 1756-EN4TR – Actualizar a las versiones V5.001 y posteriores.
- 1756-EN2T Serie D, 1756-EN2F Serie C, 1756-EN2TR Serie C, 1756-EN3TR Serie B y 1756-EN2TP Serie A – Actualizar a la versión V12.001 y posteriores.

> *«Esta vulnerabilidad tenía el riesgo de exponer sistemas de control críticos a accesos no autorizados a través del protocolo CIP originados desde ranuras de chasis no confiables»*, comentó Brizinov.