Microsoft ha identificado dos fallos de seguridad en Rockwell Automation PanelView Plus que pueden ser utilizados por atacantes remotos no autenticados para ejecutar código arbitrario y causar una condición de denegación de servicio (DoS).

> *«La vulnerabilidad de [ejecución remota de código] en PanelView Plus implica dos clases personalizadas que pueden ser aprovechadas para cargar y ejecutar una DLL maliciosa en el dispositivo»,* explicó el investigador de seguridad Yuval Gordon.
>
> *«La vulnerabilidad de DoS utiliza la misma clase personalizada para enviar un búfer manipulado que el dispositivo no puede manejar correctamente, lo que lleva a una condición de DoS.»*

Las deficiencias son las siguientes:

- CVE-2023-2071 (puntuación CVSS: 9.8): una vulnerabilidad de validación de entrada inadecuada que permite a atacantes no autenticados ejecutar código remoto mediante paquetes maliciosos manipulados.
- CVE-2023-29464 (puntuación CVSS: 8.2): una vulnerabilidad de validación de entrada inadecuada que permite a un atacante no autenticado leer datos de la memoria mediante paquetes maliciosos manipulados y provocar un DoS al enviar un paquete más grande que el tamaño del búfer.

La explotación exitosa de estos dos fallos permite a un adversario ejecutar código de forma remota o provocar la divulgación de información o una condición de DoS.

Mientras que CVE-2023-2071 afecta a FactoryTalk View Machine Edition (versiones 13.0, 12.0 y anteriores), CVE-2023-29464 afecta a FactoryTalk Linx (versiones 6.30, 6.20 y anteriores).

Es importante mencionar que los avisos sobre estos fallos fueron emitidos por Rockwell Automation el 12 de septiembre de 2023 y el 12 de octubre de 2023, respectivamente. La

Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) publicó sus propias alertas el 21 de septiembre y el 17 de octubre.

La divulgación se produce en un momento en que se cree que actores de amenazas desconocidos están explotando una vulnerabilidad crítica de seguridad recientemente revelada en HTTP File Server (CVE-2024-23692, puntuación CVSS: 9.8) para distribuir mineros de criptomonedas y troyanos como Xeno RAT, Gh0st RAT, PlugX y GoThief, este último utilizando Amazon Web Services (AWS) para robar información del host infectado.

La vulnerabilidad, descrita como un caso de inyección de plantillas, permite a un atacante remoto no autenticado ejecutar comandos arbitrarios en el sistema afectado mediante el envío de una solicitud HTTP especialmente diseñada.