Investigadores de seguridad cibernética revelaron este jueves 10 vulnerabilidades críticas, que afectan al software de automatización CODESYS. Las vulnerabilidades podrían explotarse para la ejecución remota de código en controladores lógicos programables (PLC).

> *«Para explotar las vulnerabilidades, un atacante no necesita un nombre de usuario o contraseña; tener acceso de red al controlador industrial es suficiente. La principal causa de las vulnerabilidades es la verificación insuficiente de los datos de entrada, que a su vez, puede deberse al incumplimiento de las recomendaciones de desarrollo seguro»,* dijeron los investigadores de Positive Technologies.

La compañía rusa de ciberseguridad dijo que detectó las vulnerabilidades en un PLC que ofrece WAGO, que, entre otras empresas de tecnología de automatización como Beckoff, Kontron, Moeller, Festo, Mitsubishi y HollySys, utilizan el software CODESYS para programar y configurar los controladores.

CODESYS ofrece un entorno de desarrollo para programar aplicaciones de controladores para su uso en sistemas de control industrial. La compañía de software alemana le dio crédito a Vyacheslav Moskvin, Denis Goryushev, Anton Dorfman, Ivan Kurnakov y Sergey Fedonin, de Positive Technologies, y a Yossi Reuven, de SCADAfence, por informar las vulnerabilidades.

Se identificaron seis de las fallas más graves en el componente del servidor web CODESYS v2.3, utilizado por CODESYS WebVisu para visualizar una interfaz hombre-máquina (HMI) en un navegador web.

Un adversario podría aprovechar las vulnerabilidades para enviar solicitudes de servidor web especialmente diseñadas para desencadenar una condición de denegación de servicio, escribir o leer código arbitrario hacia y desde la memoria de un sistema de tiempo de ejecución de control e incluso, bloquear el servidor web CODESYS.

Las seis vulnerabilidades fueron calificadas con la máxima puntuación, 10 de 10 en escala CVSS:

- CVE-2021-30189: Desbordamiento de búfer basado en pila
- CVE-2021-30190: Control de acceso inadecuado
- CVE-2021-30191: Copia de búfer sin verificar el tamaño de la entrada
- CVE-2021-30192: Comprobación de seguridad implementada incorrectamente
- CVE-2021-30193: Escritura fuera de los límites
- CVE-2021-30194: Lectura fuera de los límites

De forma separada, otras tres vulnerabilidades con puntaje CVSS de 8.8, reveladas en el sistema de tiempo de ejecución Control V2, podrían utilizarse para crear solicitudes maliciosas que pueden resultar en una condición de denegación de servicio o ser utilizadas para la ejecución remota de código.

- CVE-2021-30186: Desbordamiento de búfer basado en montón
- CVE-2021-30188: Desbordamiento de búfer basado en pila
- CVE-2021-30195: Validación de entrada incorrecta

Finalmente, una vulnerabilidad encontrada en la biblioteca CODESYS Control V2 Linux Sysfile (CVE-2021-30187, con puntaje CVSS 5.3), podría utilizarse para llamar a funciones de PLC adicionales, lo que a su vez permite que un atacante elimine archivos e interrumpa procesos críticos.

«Un atacante con pocas habilidades podría explotar estas vulnerabilidades», advirtió CODESYS.

> *«Su explotación puede conducir a la ejecución remota de comandos en PLC, lo que puede interrumpir los procesos tecnológicos y causar accidentes industriales y pérdidas económicas. El ejemplo más notorio de explotación de vulnerabilidades similares es el uso de Stuxnet»*, dijo Vladimir Nazarov, director de seguridad de ICS en Positive Technologies.

La divulgación de las vulnerabilidades de CODESYS llega poco después de problemas

similares que se abordaron en los PLC Siemens SIMATIC S7-1200 y S7-1500, que podrían ser explotados por los atacantes para obtener acceso de forma remota a áreas protegidas de la memoria y lograr ejecución de código no restringido y no detectado.