CODESYS lanzó parches para abordar hasta 11 vulnerabilidades de seguridad, que de ser explotadas con éxito, podrían provocar la divulgación de información y una condición de denegación de servicio (DoS), entre otras afectaciones.

> *«Estas vulnerabilidades son fáciles de explotar y pueden explotarse con éxito para causar consecuencias como la fuga de información confidencial, los PLC que ingresan en un estado de falla grave y la ejecución de código arbitrario. En combinación con los escenarios industriales en el campo, estas vulnerabilidades podrían exponer la producción industrial al estancamiento, daños a los equipos, etc.»*, dijo la compañía china de seguridad cibernética NSFOCUS.

CODESYS es un paquete de software utilizado por especialistas en automatización como entorno de desarrollo para aplicaciones de controladores lógicos programables (PLC).

Después de la divulgación responsable en septiembre de 2021 y enero de 2022, la compañía de software alemana envió correcciones la semana pasada el 23 de junio de 2022. Dos de las vulnerabilidades se calificaron como críticas, siete como altas y dos de gravedad media. Los problemas afectan de forma colectiva a los siguientes productos:

- Sistema de desarrollo CODESYS anterior a la versión V2.3.9.69
- CODESYS Gateway Client anterior a la versión V2.3.9.38
- CODESYS Gateway Server anterior a la versión V2.3.9.38
- Servidor web CODESYS anterior a la versión V1.1.9.23
- CODESYS SP Realtime NT anterior a la versión V2.3.7.30
- CODESYS PLCWinNT anterior a la versión V2.4.7.57
- CODESYS Runtime Toolkit de 32 bits completo antes de la versión V2.4.7.57

Las principales vulnerabilidades son CVE-2022-31805 y CVE-2022-31806 (puntuaciones CVSS: 9.8), que se relacionan con el uso de texto sin cifrar de contraseñas utilizadas para autenticarse antes de realizar operaciones en los PLC y una vulnerabilidad para habilitar la protección con contraseña de forma predeterminada en el sistema de tiempo de ejecución de

CODESYS Control respectivamente.

Explotar las vulnerabilidad no solo podría permitir que un atacante tome el control del dispositivo PLC de destino, sino que también podría descargar un proyecto no autorizado a un PLC y ejecutar código arbitrario.

La mayoría de las otras vulnerabilidades (desde CVE-2022-32136 hasta CVE-2022-32142) podrían ser armadas por un atacante previamente autenticado en el controlador para provocar una condición de denegación de servicio.

En un aviso separado publicado el 23 de junio, CODESYS dijo que también solucionó otras tres fallas en CODESYS Gateway Server (CVE-2022-31802, CVE-2022-31803 y CVE-2022-31804) que podrían aprovecharse para enviar solicitudes diseñadas para omitir la autenticación y bloquear el servidor.

Además de aplicar los parches de forma oportuna, se recomienda *«ubicar los productos afectados detrás de los dispositivos de protección de seguridad y realizar una estrategia de defensa en profundidad para la seguridad de la red».*