Un conjunto de 16 vulnerabilidades de seguridad de alta gravedad ha sido revelado en el kit de desarrollo de software (SDK) CODESYS V3, que podría dar lugar a la ejecución remota de código y la denegación de servicio en condiciones específicas, planteando riesgos para los entornos de tecnología operativa (OT).

Las vulnerabilidades, identificadas desde CVE-2022-47378 hasta CVE-2022-47393 y conocidas como CoDe16, tienen una puntuación CVSS de 8.8, a excepción de CVE-2022-47391, que tiene una calificación de gravedad de 7.5. Doce de estas vulnerabilidades se relacionan con desbordamientos de búfer.

> *«La explotación de las vulnerabilidades descubiertas, que afectan a todas las versiones de CODESYS V3 anteriores a la versión 3.5.19.0, podría poner en riesgo la infraestructura de tecnología operativa (OT) ante ataques como la ejecución remota de código (RCE) y la denegación de servicio (DoS)»,* informó Vladimir Tokarev de la Comunidad de Inteligencia de Amenazas de Microsoft en un informe.

Aunque aprovechar con éxito estas vulnerabilidades requiere autenticación de usuario, así como un conocimiento profundo del protocolo patentado de CODESYS V3, los problemas podrían tener consecuencias graves, como la ocurrencia de apagones y la manipulación maliciosa de procesos críticos de automatización.

Los defectos de ejecución remota de código, en particular, podrían ser explotados para introducir accesos traseros en dispositivos de tecnología operativa (OT) e interferir en el funcionamiento de controladores lógicos programables (PLCs) de una manera que podría allanar el camino para el robo de información.

> *«Explotar las vulnerabilidades requiere autenticación de usuario, así como evadir las medidas de Prevención de Ejecución de Datos (DEP) y la Aleatorización del Diseño del Espacio de Direcciones (ASLR) utilizadas por ambos PLC»,* explicó Tokarev.

Para sortear la barrera de autenticación de usuario, se utiliza una vulnerabilidad conocida (CVE-2019-9013, puntuación CVSS: 8.8) para obtener credenciales a través de un ataque de repetición contra el PLC, seguido de aprovechar los defectos para desencadenar un desbordamiento de búfer y tomar el control del dispositivo.

Se publicaron parches para estos defectos en abril de 2023. A continuación, se presenta una breve descripción de los problemas:

- CVE-2022-47378 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas con contenido inconsistente pueden provocar que el componente CmpFiletransfer lea internamente desde una dirección no válida, lo que podría desencadenar una condición de denegación de servicio.

- CVE-2022-47379 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas pueden ocasionar que el componente CmpApp escriba datos controlados por un atacante en la memoria, lo que podría llevar a una condición de denegación de servicio, sobrescritura de memoria o ejecución remota de código.

- CVE-2022-47380 y CVE-2022-47381 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas pueden hacer que el componente CmpApp escriba datos controlados por un atacante en la pila, lo que podría resultar en una condición de denegación de servicio, sobrescritura de memoria o ejecución remota de código.

- CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389 y CVE-2022-47390 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas pueden llevar al componente CmpTraceMgr a escribir datos controlados por un atacante en la pila, lo que podría derivar en una condición de denegación de servicio, sobrescritura

de memoria o ejecución remota de código.

- CVE-2022-47385 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas pueden causar que el componente CmpAppForce escriba datos controlados por un atacante en la pila, lo que podría resultar en una condición de denegación de servicio, sobrescritura de memoria o ejecución remota de código.

- CVE-2022-47391 – Solicitudes de comunicación manipuladas pueden llevar a los productos afectados a leer internamente desde una dirección no válida, lo que podría derivar en una condición de denegación de servicio.

- CVE-2022-47392 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas con contenido inconsistente pueden causar que los componentes CmpApp/CmpAppBP/CmpAppForce lean internamente desde una dirección no válida, lo que podría derivar en una condición de denegación de servicio.

- CVE-2022-47393 – Tras una autenticación exitosa, solicitudes de comunicación específicas manipuladas pueden hacer que el componente CmpFiletransfer desreferencie direcciones proporcionadas por la solicitud para acceso de lectura interna, lo que podría llevar a una situación de denegación de servicio.

> *«Con CODESYS siendo empleado por muchos proveedores, una sola vulnerabilidad puede afectar a diversos sectores, tipos de dispositivos y áreas, sin mencionar las múltiples vulnerabilidades»,* expresó Tokarev.

> *«Los actores de amenazas podrían desencadenar un ataque de denegación de*

> *servicio contra un dispositivo que utilice una versión vulnerable de CODESYS para cerrar operaciones industriales o aprovechar las vulnerabilidades de ejecución remota de código para implantar una puerta trasera y robar datos confidenciales, interferir con operaciones o forzar a un PLC a funcionar de manera peligrosa».*