Schwachstellen in der Automatisierungslösung CODESYS

Bei CODESYS handelt es sich um eine weitgehend plattformunabhängige Automatisierungslösung, die sowohl eine Laufzeitumgebung für Industriesteuerungen bietet, als auch eine Programmierumgebung mit den passenden Schnittstellen zur Verwaltung der Anlagen. Das Produkt kommt auf Geräten verschiedener Hersteller zum Einsatz und wird mit umfassenden Funktionen hinsichtlich der IT-Sicherheit beworben.

Im Zuge einer Forschungsarbeit wurden mehrere Schwachstellen in der Plattform identifiziert und dem Hersteller 3S-Smart Software Solutions GmbH gemeldet.

Probleme in der Sitzungsverwaltung ermöglichen eine vergleichsweise einfache Übernahme fremder Sitzungen durch einen Angreifer, der eine Verbindung mitlesen kann. Benutzersitzungen sind außerdem anfällig für Denial-of-Service-Angriffe. Andere Schwachstellen ermöglichen empfindliche Störungen der auf CODESYS-Steuerung ausgeführten Applikationen. Ferner führt ein fehlerhaft implementiertes Rechtekonzept im Zusammenspiel mit einer nicht konsequent umgesetzten Signaturprüfung bei SPS-Applikationen zu Szenarien, bei denen ein Angreifer die volle Kontrolle über eine Steuerung übernehmen kann.

Einzelne Schwachstellen wurden vom Hersteller bereits behoben (siehe Links), während für andere Befunde noch die entsprechenden Updates ausstehen.

https://www.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-02_CDS-65123.pdf (CVE-2019-9010)
https://www.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-03_CDS-64208.pdf (CVE-2019-9012)