**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-Steuerungen 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.

Ein weiteres Problem besteht in der Übermittlung von Benutzerpasswörtern beim Login. Diese werden mit einem fest vorgegebenen Kennwort verschlüsselt, das bereits von mehreren Forschern durch Reverse-Engineering offengelegt wurde. Damit lassen sich die Klartextpasswörter anhand eines mitgelesenen Login-Vorgangs einfach ermitteln. Diese Problematik lässt sich nur durch die Verwendung von gesicherten TLS-Verbindungen lösen, was jedoch nicht von allen SPS-Herstellern unterstützt wird.

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)
https://www.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-04_CDS-65847.pdf (CVE-2019-9008)
https://www.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-06_CDS-65149.pdf (CVE-2019-9009)
https://www.codesys.com/fileadmin/data/customers/security/2019/Advisory2019-08_CDS-62813.pdf (CVE-2019-9013)