Schwachstellen in der Siemens LOGO!8-Steuerung

Bei Siemens LOGO! handelt es sich um eine Reihe von speicherprogrammierbaren Steuerungen, die primär für kleine Automatisierungsaufgaben gedacht sind. Zusätzlich stellt Siemens entsprechende Software zur Konfiguration und Programmierung der Geräte bereit.

Im Rahmen einer universitären Abschlussarbeit in Kooperation mit der Ruhr-Universität Bochum wurden Schwachstellen in dem zur Kommunikation zwischen Software und Steuerung verwendeten Protokoll sowie hinsichtlich des integrierten Webservers identifiziert und an den Hersteller Siemens AG gemeldet.

Ein Fehler in der Implementierung des Protokolls ermöglicht einem nicht authentifizierten Angreifer mit Zugriff auf Port 10005/tcp die Provokation eines Denial-of-Service, indem speziell konstruierte Pakete an die Steuerung gesendet werden. Weitere gemeldete Schwachstellen betreffen die Sicherheit der vom integrierten Webserver verwendeten Verschlüsselung.

Während die erste Schwachstelle bereits mit einem Firmware-Update adressiert wurde [1], stehen für weitere gemeldete Schwachstellen noch die entsprechenden Updates aus.

[1] https://cert-portal.siemens.com/productcert/pdf/ssa-774850.pdf (CVE-2019-6571)