Sicherheit industrieller Steuerungssysteme: Siemens Simatic-S7 1200

Ch. Weis

Abstract

Das Projekt beschäftigt sich mit der Sicherheit und verschiedenen Angriffsvektoren eines Simatic-S7 Steuerungssystem. Verwendet wurde ein Gerät der 1200er Reihe.

1 Einleitung

Heutzutage sind intelligente Steuerungssysteme vonnöten um in Industrieanlagen effizient zu produzieren. Sicherheit spielt dabei immer eine wichtige Rolle wie man zum Beispiel beim Virus Stuxnet erkennt. Sicherheit heißt nicht nur den Schaden an Mensch und Maschine verhindern, sondern auch Cybersicherheit. In einer so vernetzten Welt wie der in der wir heute leben können fehlende Maßnahmen im Bereich der Cybersecurity gefährlich sein. Insbesondere sind die Systeme von Siemens gefährdet, da diese in der Branche Marktführer sind. Daher ist es erforderlich, sicherheitsrelevante Eigenschaften dieser Geräte genau zu kennen. Ziel der vorliegenden Arbeit ist es, den aktuellen Sicherheitsstand eines solchen Systems zu untersuchen.

2 Werkzeuge und Materialien

Verwendet wurden die Tools Nmap und Wireshark.

Nmap: Nmap, von Gordon Lyon entwickelt, ist ein Tool um Netzwerke oder auch einzelne IP-Adressen zu scannen, um Services und Ports zu finden. Nmap zeigt die offenen Ports mit den jeweiligen Protokollen an. [4]

Wireshark: Wireshark, von der Wireshark-Community entwickelt, wird verwendet um Netzwerkverbindung zu überwachen und mitzuschneiden. Hiermit kann man IP-Adressen, MAC-Adressen und Paketinformationen aus einem Netzwerk mitschneiden und abhören. [5]

S7-1200: Der Siemens Simatic-S7 1200 mit 1212C AC/DC/RLY CPU wurde als Ziel-Gerät ausgewählt, da er ein häufig verwendetes Gerät der Industrie ist. Siemens ist in diesem Gebiet weltweiter Marktführer. Das S7-System wird zu Automation von großen Industrieanlagen verwendet, indem es selber auf Daten von Sensoren reagiert, wenn es vorher einprogrammiert wurde. Das System kann über verschiedene Programme gesteuert werden. z.B.: TIA und STEP7 [3] [1] [2] [3] [5] [4]

3 Vorgehen

Zuerst wird das Gerät mit Nmap gescant um herauszufinden welche Protokolle von dem Gerät gesprochen werden. Dafür wurde der "-sS"-Scan verwendet und mit dem "-sV"-Scan ergänzt. "-sS" scannt das Ziel-Gerät im "stealthy"-Modus und "-sV" scannt nach der Version verwendeter Services. Die Scans wurden mit Wireshark mitgeschnitten und überwacht. Nun wurden zwei offenen Ports gefunden und das Protokoll anzeigt.

```
PORT  STATE  SERVICE
102/tcp  open ios-tsap
4840/tcp  open opcua
```

Nun wurden Implementierungen für die verschiedenen Protokolle gesucht. Gefunden wurde bei der Recherche nur ein Verweis auf eine Schwachstelle (CVE-2019-13945) mit dem Protokoll opcua, welches in dem Gerät vorhanden seien soll. Die Schwachstelle befindet sich im Bootloader und kann wärend des Bootvorgangs in einem Zeitfenster von genau einer halbe Sekunde ausgenutzt werden. Der Bootloader muss die Version 4.2.1 vorweisen. Wärend des Zeitfensters kann man dann ein Payload aufspielen und es danach ausführen. Auch außerhalb des Zeitfensters. Um eine Verbindung mit dem S7 1200 aufzubauen muss der Computer über ein Adapter für serielle Verbindungen verfügen. Auf dem mir zugänglichen Gerät aber befindet sich eine neuere Bootloader Version, in der der Exploit nicht mehr vorhanden ist. Auf verschiedenen Websites ist kein Verweis auf das Erscheinungsdatum verschiedener Bootloaderversionen. Einzig die Firmware wird aufgeführt, jedoch ohne Erscheinungsdaten. Darauf wurde versucht das Siemens Simatic-Step7 System

auf einem Windowsrechner zu installieren. Die Sicherheitslücke ließ sich aber nicht auf dem vorliegenden Gerät reproduzieren. [5] [4]

4 Schlussfolgerung

Die oben genannte Schwachstelle (CVE-2019-13945) konnte nicht nachgewiesen werden. Trotzdem ist diese Schwachstelle auf dem vorliegenden Gerät nicht zu unterschätzen, da doch große Schäden bei älteren Geräten auftreten können, wenn diese Schwachstelle von Angreifern gefunden wird.

References

[1] Patrick Beuth (Spiegel Netzwelt). "Stuxnet"-Entdeckung vor zehn JahrenlDie erste Cyberwaffe und ihre Folgen, 2020. https://www.spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147.

[2] RUB-SysSec. Siemens s7 plcs bootloader arbitrary code execution utility, 2020. https://github.com/RUB-SysSec/SiemensS7-Bootloader.

[3] Unbekannt. Siemens Umsatz 2019-2022, 2022. https://de.statista.com/statistik/daten/studie/316295/umfrage/umsatz-von-siemens-nach-quartalen/.

[4] Unbekannt. Nmap, Unbekannt. https://nmap.org/.

[5] Unbekannt. Wireshark, Unbekannt. https://www.wireshark.org/.