西门子S7-300,数字输入 SM 321, 光隔离西门子代理商

产品名称	西门子S7-300,数字输入 SM 321, 光隔离西门子代理商
公司名称	湖南西控自动化设备有限公司
价格	.00/件
规格参数	西门子:S7300 PLC:6ES73211BH020AA0 德国:16数字量输入, 24 V DC, 1
公司地址	中国（湖南）自由贸易试验区长沙片区开元东路1306号开阳智能制造产业园（一期）4#栋301
联系电话	17838383235 17838383235

产品详情

工控安全之西门子plc漏洞复现

0x01 工业控制简述

工业控制系统(Industrial Control Systems,ICS,简称工控系统),是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。因工控系统具备实时性、高适应性、高可用性，其在电厂中有着广泛的应用。

0x02 工控渗透测试探究分析

上文简述了工控系统以及其广泛的应用，与之相对比的是工控系统的脆弱性，由于工控产品及系统在设计之初并未着重考虑安全性或多或少存在着一定的漏洞，而其长达数年的建设使用周期又导致难以更新维护，再加上工控联网化智能化的浪潮导致如今的工控系统安全性越来越应该值得被关注。在种种基础上，结合自身工作要求，以五楼发电环境为例，我进行了工控渗透测试的探究分析。

五楼发电环境采用的为S7-300型号的PLC，其使用西门子专有的协议S7Comm协议，由于该协议未对操作进行校验，且未针对反重放攻击设置有效的保护机制，构造相应脚本具备利用空间，现利用ISF工具有关模块完成对PLC启停的控制，进行漏洞复现。

0x03 西门子S7Comm协议系列PLC漏洞复现

ISF是一个基于Python开发的适合工控的漏洞利用框架，其核心的工控协议模块中就支持S7COMM协议等。ISF可以在kali中安装，需要的python依赖环境有gnureadline(OSX only)、requests、paramiko、beautifulsoup4、pysnmp、python-nmap以及scapy。值得注意的是，安装时需确认kali中python与pip的版本在同一代，

接下来给出其安装运行指令：

git clone https://github.com/dark-lbp/isf/

cd isf

pip install -r requirements.txt

python isf.py

ISF漏洞利用框架安装成功后，运行界面如下：

ISF的具体使用方式和metasploit非常相似，可以使用help指令查看说明列表，通过use加tab键的方式查看可用模块，使用showoptions查看参数，设定参数后即可对目标PLC进行渗透攻击，此处使用的为其exploits/plcs/siemens/s7_300_400_plc_control模块。值得注意的是，与主机漏洞渗透测试相同，此处同样需要先禁用无线，配置与目标PLC同网段的IP。漏洞复现的具体步骤如下：

可以看到，此处已成功利用ISF实现了对PLC启停的控制，现场PLC设备也从显示为绿色的RUN运行灯光变为了显示为黄色的STOP运行灯光。

运行前：

运行后：

0x04 西门子S7Comm协议系列PLC漏洞修复建议

综上所述已完成了对西门子S7Comm协议系列PLC漏洞的复现，现给出修复建议：

（1）升级相关协议；

（2）针对CPU模块中protection选项卡设置密码进行口令保护。

目前工控漏洞利用框架ISF相关模块模拟西门子S7Comm协议编写的payload仅能实现对PLC的启停控制，下一步可以尝试深入分析西门子S7Comm协议，编写相关payload并设计脚本实现例如对PLC下层控制器的操控等更深层次利用。

本文参考文献：