

GE_Proficiency_Machine_Edition_Vuln

A PoC of GE Proficy Machine Edition 8.0

Proficy Machine Edition is a software that deploys HMI, motion, and multi-target control, providing a common user interface, drag-and-drop editing, and a rich set of development tools, widely used in Industrial Control System.

Reference: [Proficy Machine Edition](#)

This repository gives the PoC that crashes the program! If you need the details, please contact me(dliangfun@gmail.com).

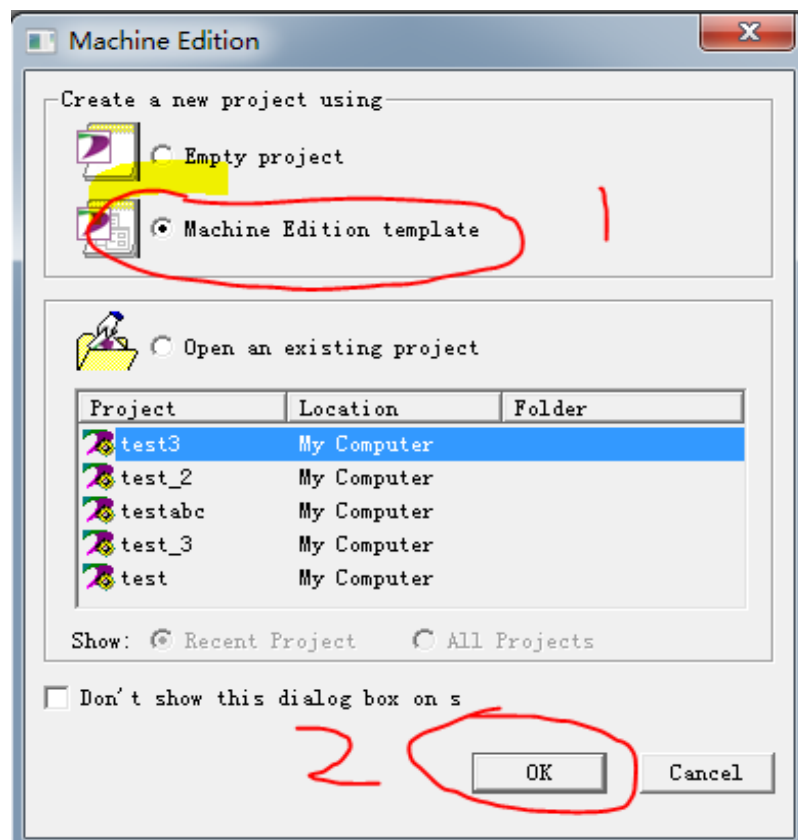
PoC deploy instruction

Proficy Machine Edition run on desktop (eg. Win7), connecting to a device such as **GE RX7i**. Attacker can exploit MITM taking control of communication traffic, but on demonstration, attacker was on a role of Proxy. Therefore, **poc.py** is the attacker's program.

Steps

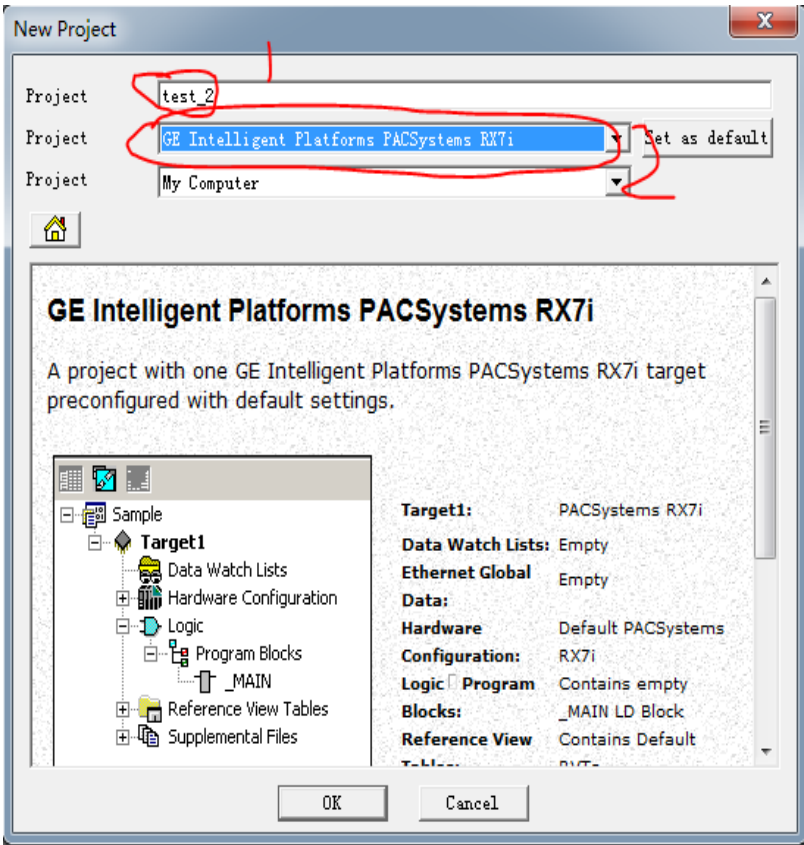
Create a new Project

- 1. Create a new project using **Machine Edition template**



- 2. Name the project as **test_2** and choose device **RX 7i**

Note that the project name must be named as **test_2** for the correctly reproducing the vulnerability.



• 3.Configure IP address

Proficy Machine Edition should be configured correct address with proxy program's IP, proxy program is act as a device.

Set **Physical Port** as **ETHERNET** and **IP Address** as **127.0.0.1**.

Inspector	
Target	
Name	Target1
Type	GE IP Controller
Description	
Documentation Address	
Family	PACSystems RX7i
Controller Target Name	test21
Update Rate (ms)	250
Sweep Time (ms)	Offline
Controller Status	Offline
Scheduling Mode	Normal
Force Compact PVT	True
Enable Shared Variables	False
Enhanced Security	False
Physical Port	ETHERNET
IP Address	127.0.0.1
Additional Configuration	
Inspector	

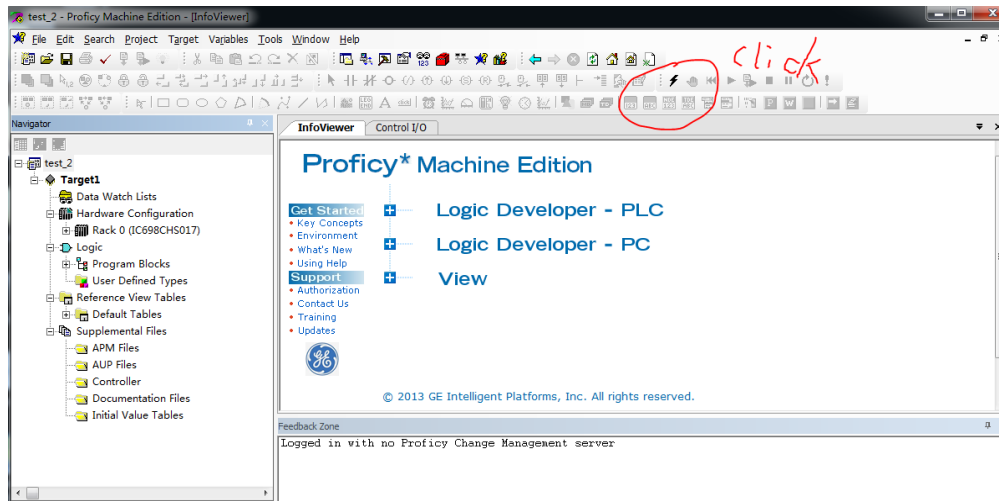
Run the poc.py

- 4.The proxy program poc.py was run, and listen to port 18245

Operate the GUI

- 5.Click the connect button as following

Operation as following:



Finally software will crash as following:

