Security notification – Modicon™ Quantum PLC (ICS-ALERT-12-020-03B)

April 5, 2012

Schneider Electric® has become aware of the release of a metasploit module allowing a user to send a stop command to or modify the PLC program of a Modicon Quantum PLC.

This tool replicates the behavior existing inside Unity™ Pro software today.

The ability to send commands from Unity Pro software or using UMAS protocol to the controller was already identified in ICS-ALERT-12-020-03A and a response is available in Schneider Electric Resolution RES207378. An extract from this resolution is provided below:

4) No Authentication between Unity Software and the PLC

The transmission of Modbus™ function codes 125 and 126 from the Unity Pro software to the PLC allows for control of the application and programming functions. To limit access to these functions Schneider Electric recommends:

a) Implementing the Access Control List for port 502 (Modbus) on the Messaging tab of the Ethernet communications interface configuration, limiting access to only authorized IP addresses.

b) Limiting access to the module using an external firewall.

c) Setting of the memory protect switch on the PLC to prevent remote modification of the program.

5) General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://www.citect.schneider-electric.com/documents/STN_Ethernet.pdf

Support

If you are unsure of whether you could be affected by this vulnerability or if you have any questions on this issue please contact your local Schneider Electric support center.