Digital Bond releases Metasploit tools to demonstrate vulnerabilities in Quantum HTTP passwords and Ethernet/IP protocol

February 16, 2012

On February 14, 2012, security research and consulting company, Digital Bond, released Metasploit modules designed to allow an attacker to execute attacks against an Ethernet/IP device and Schneider Electric PLCs. Further information on the two Metasploit modules is below:

“modiconpass”

This Metasploit module is designed to retrieve the list of HTTP username/passwords from the module, using system accounts that are built into the PLC communications interfaces to enable automatic services. These accounts are discussed in RESL206895, RESL207378 and in a document making recommendations on specific firewall rules to protect the modules that will be released as a resolution in the coming days. In addition, they are covered in documents from ICS-CERT, ICS-Alert-12-20-03 and ICS-ALERT-11-346-01. Schneider Electric is investigating methods to modify the system operation to limit the scope of these accounts. Prior to any changes, Schneider Electric recommends following a Defense in Depth approach to limit the accessibility of the FTP server from the network (to prevent retrieval of the passwords) and also to limit HTTP access to authorized devices only. This can be accomplished through the use of a Hirschmann Tofino firewall. Instructions on the use of this device to mitigate the vulnerabilities can be found at Mitigation of vulnerabilities.

“ethernetip-multi.rb”

This Metasploit module is designed to issue "Stop CPU" and "Reboot Ethernet Controller" commands to a device. Schneider Electric PLC devices do not implement the "Stop CPU" command over Ethernet/IP and so do not suffer from this vulnerability. Schneider Electric PLC devices disable the "Reboot Ethernet Controller" command when using the default configuration, and so do not suffer from this vulnerability unless the user has selected to enable this option, or the module is in an un-configured state.

ODVA has also released a statement to its members regarding this module.

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:

How can I….protect a system from Cyber Security attacks?

If you have any questions on these Metasploit modules please contact your local Schneider Electric support center.