



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-020-03B—SCHNEIDER ELECTRIC MODICON QUANTUM MULTIPLE VULNERABILITIES

UPDATE B

April 09, 2012

ALERT

SUMMARY

This Alert Update is a follow-up to the original ICS-CERT Alert titled “ICS-ALERT-12-020-03—Schneider Electric Modicon Quantum Multiple Vulnerabilities” that was published January 20, 2012, on the ICS-CERT web page.

ICS-CERT is aware of a public report of multiple vulnerabilities affecting Schneider Electric Modicon Quantum PLC. According to this report, these vulnerabilities are exploitable through backdoor accounts (previously disclosed),^a malformed HTTP or FTP requests, or cross-site scripting (XSS).

Proof-of-concept (PoC) exploit code has been released targeting the password storage on the Schneider Electric Modicon Quantum PLC. This exploit module retrieves stored username and passwords for the webserver login and an additional password that may be used to modify control operations via the web interface.

----- Begin Update B Part 1 of 2 -----

Reid Wightman of Digital Bond has released Metasploit modules to exploit the vulnerabilities outlined in this alert.

Newly Released Metasploit modules^b:

- **modicon_command**—allows a remote, unauthenticated user to issue stop and start commands. If an attacker has access to the Modbus TCP port, an attacker can simply stop or start the CPU without authentication.
- **modicon_stux_transfer**—allows a remote, unauthenticated user to download and upload possibly modified ladder logic via Modbus.

----- End Update B Part 1 of 2 -----

a. http://www.us-cert.gov/control_systems/pdf/ICSA-12-018-01.pdf website last accessed April 09, 2012.

b. <https://community.rapid7.com/community/metasploit/blog/2012/04/05/metasploit-update> Website last accessed April 09, 2012.

This product is provided subject only to the Notification Section as indicated here: <http://www.us-cert.gov/privacy/>



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTROL SYSTEMS SECURITY PROGRAM

This report is based on information presented by the Project Basecamp team during Digital Bond’s SCADA Security Scientific Symposium (S4) on January 19, 2012. The vulnerability information is based on research conducted by Rubén Santamarta; the information was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified Schneider Electric of the report and has asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is issuing this alert to provide preliminary notice of the reported vulnerable products and to begin identifying baseline mitigations that can reduce the risk of cybersecurity attacks that may exploit these vulnerabilities.

The presentation summarized the following vulnerabilities without going into detail:

Vulnerability Type	Exploitability	Impact
No authentication between Unity software and PLC	Remote	Denial of Service / Possible Remote Code Execution
Backdoor accounts ^a	Remote	Access system as user or administrator
HTTP Server buffer overflows	Remote	Denial of Service
FTP Server buffer overflows	Remote	Denial of Service
XSS	Remote	Unknown

In addition, the Project Basecamp team identified approximately 200 instances of Modicon Quantum PLCs directly facing the Internet. ICS-CERT reminds users that the use of readily available and generally free search tools (such as SHODAN and ERIPP) significantly reduces time and resources required to identify Internet facing control systems. In turn, hackers can use these tools combined with the exploit modules to identify and attack vulnerable control systems. Conversely, owners and operators can also use these same tools to audit their assets for unsecured Internet facing devices. For more information, ICS-CERT recommends reviewing: [ICS-ALERT-11-343-01—Control System Internet Accessibility](#).

Please report any cyber issues affecting control systems to ICS-CERT.

Schneider Electric is a manufacturer and integrator of energy management equipment and software. Its systems are found in the energy, manufacturing, building automation, and information technology, with operations in over 100 countries worldwide. The Schneider Electric Modicon PLC line contains many different devices designed for different uses and environments.

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher to identify mitigations.



ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM CONTROL SYSTEMS SECURITY PROGRAM

----- Begin Update B Part 2 of 2 -----

Schneider Electric reminds users that the following features are provided to restrict access and prevent modification of the PLC program.

- Access Control List. The Ethernet modules of the PLC support an Access Control List that can be enabled on the module configuration screen to restrict access via Modbus/UMAS protocols (Port 502/TCP) to configured IP addresses only.
- Memory Protect Key Switch. The Quantum PLCs provide a key switch located on the front panel that allows a user to protect the PLC program from modification. When set to the Memory Protect position, the PLC program cannot be modified; however, SCADA and other devices are still permitted to send commands to the PLC variables.
- PLC Memory Card. Programs stored on a memory card provide write protection via a switch on the memory card to protect the PLC program from modification. When set to the Memory Protect position, the PLC program cannot be modified; however, SCADA and other devices are still permitted to send commands to the PLC variables.

These features are described in the following resolution from Schneider Electric - [RESL207378](#).

----- End Update B Part 2 of 2 -----

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.^c
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.^d

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

c. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed April 09, 2012.

d. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 09, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS -CERT CONTACT

ICS-CERT Operations Center

1-877-776-7585

ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org document FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.