ICS-CERT ALERT

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

UPDATE A

February 14, 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).

--------- Begin Update A Part 1 of 1 --------

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.

--------- End Update A Part 1 of 1 ----------

This report is based on information presented by the Project Basecamp team during Digital Bond's SCADA Security Scientific Symposium (S4), on January19, 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:

a. http://www.us-cert.gov/control_systems/pdf/ICSA-12-018-01.pdf website last accessed February 14, 2012.

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 two hundred 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 useful mitigations.

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.[b]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed February 14, 2012.

- 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.*[c]

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.

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.

c. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 14, 2012.