ICS-CERT ALERT

ICS-ALERT-11-346-01—SCHNEIDER ELECTRIC QUANTUM ETHERNET MODULE MULTIPLE VULNERABILITES

December 12, 2011

ALERT

SUMMARY

On December 12, 2011, independent security researcher Rubén Santamarta publicly announced details of multiple vulnerabilities affecting the Schneider Electric Quantum Ethernet Module. Prior to publication, Mr. Santamarta notified ICS-CERT of the vulnerabilities. ICS-CERT is coordinating mitigations with Mr. Santamarta and Schneider Electric. Schneider has produced a fix for two of the reported vulnerabilities and is continuing to develop additional mitigations.

Multiple hardcoded credentials are revealed in Mr. Santamarta's report that enable access to the following services:

- Telnet port – May allow remote attackers the ability to view the operation of the module's firmware, cause a denial of service, modify the memory of the module, and execute arbitrary code.
- Windriver Debug port - Used for development; may allow remote attackers to view the operation of the module's firmware, cause a denial of service, modify the memory of the module, and execute arbitrary code.
- FTP service – May allow an attacker to modify the module website, download and run custom firmware, and modify the http passwords.

ICS-CERT is currently coordinating with Schneider Electric to develop mitigations. Additional information regarding the impact and mitigations will be issued as it becomes available.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

AFFECTED PRODUCTS

Quantum

140NOE77101 Firmware Version 4.9 and all previous versions.

140NOE77111 Firmware Version 5.0 and all previous versions.

140NOE77100 Firmware Version V3.4 and all previous versions.

140NOE77110 Firmware Version V3.3 and all previous versions.

140CPU65150 Firmware Version V3.5 and all previous versions.

140CPU65160 Firmware Version V3.5 and all previous versions.

140CPU65260 Firmware Version V3.5 and all previous versions.

Premium

TSXETY4103 Firmware Version V5.0 and all previous versions.

TSXETY5103 Firmware Version V5.0 and all previous versions.

TSXP571634M Firmware Version V4.9 and all previous versions.

TSXP572634M Firmware Version V4.9 and all previous versions.

TSXP573634M Firmware Version V4.9 and all previous versions.

TSXP574634M Firmware Version V3.5 and all previous versions.

TSXP575634M Firmware Version V3.5 and all previous versions.

TSXP576634M Firmware Version V3.5 and all previous versions.

M340

BMXNOE0100 Firmware Version V2.3 and all previous versions.

BMXNOE0110 Firmware Version V4.65 and all previous versions.

BMXP342020 Firmware Version V2.2 and all previous versions.[a]

BMXP342030 Firmware Version V2.2 and all previous versions.[a]

STB DIO

STBNIC2212 Firmware Version V2.10 and all previous versions.

STBNIP2311 Firmware Version V3.01 and all previous versions.

STBNIP2212 Firmware Version V2.73 and all previous versions.

a. These products are only affected by the FTP and hard-coded credential vulnerabilities.

MITIGATION

Schneider Electric has created a fix for the Telnet and Windriver debug port vulnerabilities for the BMXNOE0100 and 140NOE77101 modules, which will be published on the Schneider website. This fix removes the Telnet and Windriver services from the modules. Organizations need to evaluate the impact of removing these services prior to applying this fix. ICS-CERT will provide additional information as mitigations become available for other identified vulnerabilities.

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.
- 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

b. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed December 12, 2011

c. Control Systems Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 12, 2011.

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 declines attribution. 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.