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

ICS-CERT ADVISORY

ICSA-12-018-01—SCHNEIDER ELECTRIC QUANTUM ETHERNET MODULE HARD-CODED CREDENTIALS

January 18, 2012

OVERVIEW

This Advisory is a follow-up to the original ICS-CERT Alert titled “ICS-ALERT-11-346-01 - Schneider Quantum Ethernet Module Credentials” that was published December 12, 2011, on the ICS-CERT web page.

On December 12, 2011, independent security researcher Rubén Santamarta publicly announced information regarding hard-coded credentials in the Schneider Electric Quantum Ethernet Module. The credentials publicized grant access to the Telnet port, Windriver Debug port, and the FTP service. Prior to publication, Mr. Santamarta coordinated these vulnerabilities with ICS-CERT.

ICS-CERT has coordinated with Schneider Electric, and they have produced a patch for a portion of the reported vulnerabilities. Schneider Electric is continuing to develop additional updates for the remaining reported vulnerabilities.

Additional information regarding mitigations will be issued as it becomes available.

AFFECTED PRODUCTS

The following products and versions are affected:

Quantum

140NOE77101 Firmware V4.9 and all previous versions.

140NOE77111 Firmware V5.0 and all previous versions.

140NOE77100 Firmware V3.4 and all previous versions.

140NOE77110 Firmware V3.3 and all previous versions.

140CPU65150 Firmware V3.5 and all previous versions.

140CPU65160 Firmware V3.5 and all previous versions.

140CPU65260 Firmware V3.5 and all previous versions.

140NOC77100 Firmware V1.01 and all previous versions.

140NOC77101 Firmware V1.01 and all previous versions.

Any available conformal-coated versions of the above part numbers.

Premium

TSXETY4103 Firmware V5.0 and all previous versions.

TSXETY5103 Firmware V5.0 and all previous versions.

TSXP571634M Firmware V4.9 and all previous versions.

TSXP572634M Firmware V4.9 and all previous versions.

TSXP573634M Firmware V4.9 and all previous versions.

TSXP574634M Firmware V3.5 and all previous versions.

TSXP575634M Firmware V3.5 and all previous versions.

TSXP576634M Firmware V3.5 and all previous versions.

TSXETC101 Firmware V1.01 and all previous versions.

Any available conformal-coated versions of the above part numbers.

M340

BMXNOE0100 Firmware V2.3 and all previous versions.

BMXNOE0110 Firmware V4.65 and all previous versions.

BMXNOC0401 Firmware V1.01 and all previous versions.

The following products are affected by the FTP Service vulnerabilities only (not affected by Telnet or Windriver Debug vulnerabilities):

STBNIC2212 Firmware V2.10 and all previous versions.

STBNIP2311 Firmware V3.01 and all previous versions.

STBNIP2212 Firmware V2.73 and all previous versions.

BMXP342020 Firmware V2.2 and all previous versions.

BMXP342030 Firmware V2.2 and all previous versions.

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to gain elevated privileges, to load a modified firmware, or to perform other malicious activities on the system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Schneider Electric is a manufacturer and integrator of energy management and industrial automation systems, equipment, and software. The affected Schneider Electric systems are found primarily in energy, manufacturing, and infrastructure applications. Schneider Electric reports operations in over 100 countries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

HARD-CODED CREDENTIALS

Mr. Santamarta's report revealed multiple hard-coded credentials 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.

CVE-2011-4859[a] has been assigned to this vulnerability group. A CVSS V2 base score of 10 has also been assigned.

[a] http://web nvd nist.gov/view/vuln/detail?vulnId=CVE-2011-4859 , website last accessed January 10, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level could exploit these vulnerabilities.

MITIGATION

Schneider Electric has created a patch for the Telnet and Windriver debug port vulnerabilities for the BMXNOE01x[b]0 and 140NOE771x[c]1 modules; the patch is posted on the Schneider Electric website; http://www.schneider-electric.com/. This patch removes the Telnet and Windriver services from the modules. According to Schneider Electric, this patch will not affect the capacities/functionalities of the product or impact the performance of customer installations because the Telnet and Windriver debug services are installed only for advanced troubleshooting use and are not intended for customer use.

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.

Schneider Electric has provided the following patches on their website:

140NOE77101 Exec V5.01 for Unity Users:

http://www.global-download.schneider-electric.com/852577A4005D7372/all/C8742BA6ACE1F70185257802006DA154

140NOE77111 Exec V5.11:

http://www.global-download.schneider-electric.com/852577A4005D7372/all/8FE7D86C58AC006085257802006DCD98

BMXNOE0100 Exec V2.50 - M340 Ethernet Module:

http://www.global-download.schneider-electric.com/852577A4005D7372/all/44A8CDE36E8474B985257801006D5195

[b] "x" denotes multiple versions of the firmware.

[c] "x" denotes multiple versions of the firmware.

BMXNOE0110 Exec v5.3 - M340 Ethernet Module:

http://www.global-download.schneider-electric.com/852577A4005D7372/all/968499BE1337D4B385257802006D97C7

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

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

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams* [e] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[f] for more information on social engineering attacks.

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices html, website last accessed January 16, 2012.

[e] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 16, 2012

[f] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014 html, website last accessed January 16, 2012

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events 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.