ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-13-016-01—SCHNEIDER ELECTRIC MULTIPLE VULNERABILITIES

January 16, 2013

ALERT

SUMMARY

ICS-CERT is aware of a public report concerning multiple vulnerabilities in multiple Schneider Electric Products. These vulnerabilities were released by Arthur Gervais at the Digital Bond SCADA Security Scientific Symposium (S4) conference.

ICS-CERT notified the affected vendor of the report and asked the vendor to confirm the vulnerabilities and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

The report included vulnerability details and proof-of-concept exploit code for the following vulnerabilities:

Product	Vulnerability Type	Remotely Exploitable	Impact
BMX NOE 0110	Unauthenticated SOAP/HTTP interface	Yes	Remote code execution
Modicon M340	TCP connection resource exhaustion	Yes	Denial of Service
Magelis XBT	HMI 6001/TCP hard coded credentials	Yes	Loss of integrity
Modicon M340	Cross Site Request Forgery	Yes	Unauthorized access

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

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

MITIGATION

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

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

- Turn off or restrict FTP service when operationally possible.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a]
- 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.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[b]

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
Email: ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed January 16, 2013.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 16, 2013.

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.