ICS-CERT ALERT

ICS-ALERT-12-020-04—SCHWEITZER SEL-2032 PLAINTEXT SERVICE CRASH

January 20, 2012

ALERT

SUMMARY

ICS-CERT is aware of a report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Schweitzer Engineering Laboratories' SEL-2032 Communications Processor SCADA remote terminal unit (RTU). This report is based on research conducted by Dillon Beresford and was presented by the Project Basecamp team during the Digital Bond SCADA Security Scientific Symposium (S4) on January19, 2012. According to their findings, the RTU uses plaintext protocol for password authentication. In addition, the researchers were able to cause an intermittent crash to an unknown service through Telnet and Port 1024/TCP. Vulnerability details were released without prior coordination with either the vendor or ICS-CERT.

ICS-CERT has coordinated with Schweitzer Engineering Laboratories 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 product and to begin identifying baseline mitigations that can reduce the risk of cybersecurity attacks that may exploit these vulnerabilities.

The report included details and PoC exploit code for the following vulnerabilities:

Vulnerability Type	Exploitability	Impact
Plaintext Authentication	Local	Potential unauthorized access to system
Termination of the software	Remote	Denial of service

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

MITIGATION

ICS-CERT is currently coordinating with Schweitzer Engineering Laboratories and Dillon Beresford 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.[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.

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*.[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
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.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed January 20, 2012.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 20, 2012.