ICS-CERT ALERT

ICS-ALERT-12-020-01—S4 DISCLOSURE OF MULTIPLE PLC VULNERABILITIES IN MAJOR ICS VENDORS

January 20, 2012

ALERT

SUMMARY

This report is based on information presented by the Project Basecamp team of researchers during Digital Bond's SCADA Security Scientific Symposium (S4) on January19, 2012, without coordination with either the vendors or ICS-CERT.

The Basecamp findings include multiple zero-day vulnerabilities for several leading industrial control system (ICS) hardware Programmable Logic Controllers (PLCs). Major affected vendors include GE, Koyo, Rockwell, Schneider (Modicon), and Schweitzer. Exploit code was also released for the GE vulnerabilities. The affected PLCs are used to control functions in critical infrastructure in the chemical, energy, water, nuclear, and critical manufacturing sectors.

ICS-CERT has contacted the affected vendors about the vulnerabilities in an effort to confirm them and identify mitigations.

ICS-CERT is issuing this alert to provide preliminary notice of the reported vulnerable products and to begin identifying baseline mitigations to reduce the risk of cybersecurity attacks that may attempt to exploit these vulnerabilities.

Affected Vendors	Product
General Electric	D20/D20ME
Rockwell Automation	Allen-Bradley ConrolLogix
Rockwell Automation	Allen-Bradley MicroLogix
Schneider Electric	Modicon Quantum
Koyo	Direct LOGIC H4-ES
Schweitzer	SEL-2032

The vulnerabilities purportedly include buffer overflows, backdoors, weak authentication and encryption, and other vulnerabilities that could allow an attacker to take control of the device and interfere or halt the process it controls.

Two new Metasploit modules have been released for the GE D20/DME vulnerabilities that could allow lower skilled users to exploit these vulnerabilities. In addition, according to Basecamp researchers, additional modules targeting the other products are expected to be released soon.

This public release increases the potential for cyber attack on these devices, particularly if the devices are connected to 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.

GE, Rockwell, Schneider (Modicon), and Schweitzer PLCs are deployed extensively in the energy sector, particularly the electric grid. GE and Rockwell are also deployed extensively in the water and wastewater sector.

ICS-CERT is communicating with the researchers and affected vendors to obtain additional vulnerability details and coordinate follow-up mitigation measures. ICS-CERT has released and will continue to release separate vendor alerts and advisories once additional information becomes available (www.ics-cert.org).

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

MITIGATION

ICS-CERT is currently coordinating with the vendors and security researchers to identify useful mitigations.

ICS-CERT recommends that users take defense in depth 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.

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

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.

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