ICS-CERT ALERT

ICS-ALERT-12-020-02—ROCKWELL AUTOMATION CONTROLLOGIX MULTIPLE PLC VULNERABILITIES

January 20, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Rockwell ControlLogix, a controller product. According to this report, the vulnerability is exploitable by transmitting arbitrary commands from the PLC to the control system. This report is based on information presented by the Project Basecamp team during Digital Bond's SCADA Security Scientific Symposium (S4) on January19, 2012. Vulnerability details are based on research conducted by Rubén Santamarta. The information was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified Rockwell of the report and has asked the vendor to confirm the vulnerabilities and identify mitigations. ICS-CERT is issuing this alert to provide preliminary notice of the reported vulnerable products and to begin identifying baseline mitigations that can reduce the risk of cybersecurity attacks that may attempt to exploit these vulnerabilities.

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

Vulnerability Type	Exploitability	Impact
Improper Input Validation • **Malformed Request**	Remote	Denial of Service / Physical reboot required
Improper Input Validation • **Malformed Packet**	Remote	Denial of Service / Physical reboot required

The report also included details of methods for using legitimate commands maliciously.

Command Type	Exploitability	Impact
Interface Control	Remote	Denial of Service / Possible Man-in-the-Middle / Physical reboot required
Stop	Remote	Denial of Service / Physical reboot required

Command Type	Exploitability	Impact
Dump 1756- ENBT's module boot code	Remote	Data Leakage
Reset	Remote	Denial of Service
Firmware Upgrade	Remote	Data Integrity/Arbitrary Code Execution/Denial of Service

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

For details, please see the following Rockwell announcements:

- http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470154
- http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470155
- http://rockwellautomation.custhelp.com/app/answers/detail/a_id/470156
- http://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher 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]

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.

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.