Industry Advisory
CIP: Rockwell Automation MicroLogix Controllers Password Security and Client Software Authentication Vulnerabilities

Initial Distribution: February 3, 2010

These vulnerabilities have been publicly disclosed.

Why am I receiving this? >>
About NERC Alerts >>

Status: No Reporting is Required – For Information Only

PUBLIC: No Restrictions. Will be posted to NERC’s Web site alert page.
More on handling >>

Instructions: NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC’s Rules of Procedure, for such use as your organization deems appropriate. No particular response is necessary. This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard.

Who else will get this alert? >>
What are my responsibilities? >>

Primary Interest Groups: SCADA, EMS, Operations, Planning, and IT Security

Advisory: The ES-ISAC has been informed of two vulnerabilities in the Rockwell Automation MicroLogix family of programmable logic controllers (PLCs). The affected products are MicroLogix 1000, 1100, 1200, 1400, and 1500. Respectively, these products have the following catalog numbers: 1761-Lxxxx, 1762-Lxxxx, 1763-Lxxxx, 1764-Lxxxx, and 1766-Lxxxx.

The following two vulnerabilities have been identified:
1. **Password Security Vulnerability** – The potential exists for a highly skilled, unauthorized person with specific tools, know-how and access to the Product or the control system communication link, to intercept and decipher the Product's password and potentially make unauthorized changes to the Product's operation.

2. **Client Software Authentication Security Vulnerability** – The potential exists for a highly skilled, unauthorized person with specific tools, know-how and access to the Product or the control system communication link, to intercept data communications between the product and any authorized programming and configuration client to emulate the role of a trusted software client to potentially make unauthorized changes to the Product's operation.

To reduce the likelihood of an exploitation, Rockwell Automation recommends the following immediate mitigation strategies (Note: if possible, multiple, simultaneous strategies should be employed):

1. Disable where possible the capability to perform remote programming and configuration of the Product over a network to a controller by placing the controller's key switch into RUN mode.

2. Enable static protection on all critical data table files to prevent any remote data changes to critical data.

3. Restrict physical and electronic access to automation products, networks and systems to only those individuals authorized to be in contact with control system equipment.

4. Employ layered security and defense-in-depth methods in system design to restrict and control access to individual products and control networks. Refer to [http://www.ab.com/networks/architectures.html](http://www.ab.com/networks/architectures.html) for comprehensive information about implementing validated architectures designed to deliver these measures.

5. Block all traffic to the CSP, EtherNet/IP or other CIP protocol based devices from outside the Manufacturing Zone (where applicable) by restricting or blocking access to TCP and UDP Port# 2222 and Port# 44818 using appropriate security technology (e.g. a firewall, UTM devices, or other security appliance).

Rockwell Automation is addressing these security vulnerabilities in the aforementioned products, associated programming, and configuration software. Please refer to the Rockwell primary point of contact for further guidance.
The ES-ISAC estimates the risk to grid reliability from these vulnerabilities is LOW, due to no evidence of public release of exploitation code and lower deployment levels of the effected technology in the electricity sector.

**Background:** The effected products represent (53%) of the micro PLC market; however, the electricity sector is ranked seventh out of seven industries included in the market share.

Reference US-CERT Vulnerability Note: ICSC-10-014-01(FOUO)


Rockwell Automation Technote for Password Security Vulnerability in MicroLogix Controllers: [65980](#)

Rockwell Automation Technote for Client Software Authentication Security Vulnerability in MicroLogix Controllers: [65982](#)

**Contact:**

Doug Newbauer  
Alerts Manager  
609.937.3413  
doug.newbauer@nerc.net

To report any incidents related to this alert, contact:  
ES-ISAC 24-hour hotline  
609.452.1422  
esisac@nerc.com

A-2010-02-03-01

You have received this message because you are listed as the designated contact for your organization on the North American Electric Reliability Corporation's compliance registry. If believe you have received this message in error, please notify the sender immediately and delete or otherwise dispose of all occurrences or references to this email. If you have questions about your membership in this list, please contact Chris Scheetz at NERC by calling 609.452.8060 or emailing Chris directly at: chris.scheetz@nerc.net.

North American Electric Reliability Corporation  
116-390 Village Blvd.  
Princeton, NJ 08540  
609.452.8060 | [www.nerc.com](http://www.nerc.com)