Title: C4 SCADA Security Advisory – Rockwell Automation (Allen Bradley) Multiple Vulnerabilities in Micrologix 1100 & 1400 Series Controllers

Date: January 15 2010
Author: Eyal Udassin (eyal udassin c4-security com)

Background

Vendor product information, from www.ab.com :
With online editing and a built-in 10/100 Mbps EtherNet/IP port for peer-topeer messaging, the MicroLogix 1100 controller adds greater connectivity and application coverage to the MicroLogix family of Allen-Bradley controllers. This next generation controller's built-in LCD screen displays controller status, I/O status, and simple operator messages; enables bit and integer manipulation; offers digital trim pot functionality, and a means to make operating mode changes (Prog / Remote / Run).
With 10 digital inputs, 2 analog inputs and 6 digital outputs, the MicroLogix 1100 can handle a wide variety of tasks. The MicroLogix 1100 controllers also support expansion I/O. Up to four 1762 I/O modules (also used on the MicroLogix 1200 and 1400) may be added to the embedded I/O, providing application flexibility and support of up to 80 digital I/O.

Description

Due to the sensitivity of SCADA-related vulnerabilities, we can only publicly disclose that the Micrologix 1100 and 1400 controllers suffer from multiple vulnerabilities that allow unauthorized control of the PLC.
Details of these vulnerabilities will be disclosed only to legitimate parties such as asset owners (utilities), after receiving the approval of the local CERT or any other local official entity.

Impact

An attacker can exploit these vulnerabilities in order to:

- Halt the system's operation (Denial of Service)
- Gain unauthorized access with high privileges to the system
- Leverage these vulnerabilities to attempt to find additional vulnerabilities in the server to carry out the "field to field" attack vectors mentioned in C4's S4 2008 paper "Control System Attack Vectors and Examples: Field Site and Corporate Network" (http://www.c4- security.com/index-5.html).

Affected Versions

AB Micrologix 1100
AB Micrologix 1400

Workaround/Fix

Consult with Rockwell Automation or a SCADA security company on how to mitigate the found vulnerabilities by restricting access to the control network.

Additional Information

For additional information please contact us at info_at_c4-security.com.
Note that we will respond only to verified utility personnel and governmental agencies. Details of this vulnerability will be disclosed only to legitimate parties such as asset owners (utilities), after receiving the approval of the local CERT or any other local official entity.

The CVE identifier assigned to this vulnerability by CERT is CVE-2009-3739

Credit

These vulnerabilities were discovered and exploited by Eyal Udassin from C4 Security (http://www.c4-security.com).
We would like to thank Rockwell Automation and CERT for their professional handling of the vulnerability disclosure process.

C4 Security is a leader in SCADA security reviews, auditing and penetration testing.