NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Advisory

CIP: Rockwell Automation ControlLogix 1756-ENBT/A WebServer Vulnerabilities

Initial Distribution: February 13 2009

These vulnerabilities were publicly announced via US-CERT on February 5, 2009.
No known exploits currently exist.

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

Status:	**Information Only: No Reporting Required**
	**Public: No Restrictions.** **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.
Distribution:	**Initial Distribution: Primary Compliance Contacts** Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, Load Serving Entities, Distribution Providers **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	SCADA, EMS, Operations, Planning, IT Security, Users of Rockwell Automation ControlLogix 1756-ENBT/A webserver functionality.
Advisory:	The following vulnerabilities have been identified in the Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge and its embedded GoAhead WebServer: • Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge URL redirection vulnerability • Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge cross-site scripting vulnerability • The embedded GoAhead WebServer of the 1756-ENBT/A contains an information disclosure vulnerability; an attacker could potentially bypass authentication and view system configuration files or passwords ControlLogix 1756-ENBT/A mitigations: Users of ControlLogix 1756-ENBT/A are advised to immediately employ layered security and defense-in-depth methods in the design of the network architecture. Refer to Rockwell Automation's Reference Architectures for Manufacturing located at http://www.ab.com/networks/architectures.html for more information about establishing robust and secure network configurations. These potential security vulnerabilities will be addressed in a future release of the firmware for the 1756-ENBT/A, currently scheduled for July, 2009. GoAhead Web server mitigations: Users of the GoAhead WebServer are advised to strictly limit remote

access for this device to critical users. This may be done via firewall rules and router access control lists.

The ES-ISAC estimates that the risk to bulk power system reliability from this vulnerability is LOW; however technical risk to an individual facility possessing the vulnerability is MEDIUM. There is no evidence of exploitation code being released into the public.

Background:

Actions that can be taken by an attacker are:

ControlLogix 1756-ENBT/A

1. An attacker can potentially redirect a user's browser to another website and execute arbitrary JavaScript in an operator's browser.
2. This script can be used to spoof data or redirect an operator's web browser to other sites.

GoAhead WebServer

An attacker can potentially view any file on the web server including files that contain usernames and passwords.

References:

Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge cross-site scripting vulnerability VU#882619 (http://www.kb.cert.org/vuls/id/882619)
Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge URL redirection vulnerability VU#619499 (http://www.kb.cert.org/vuls/id/619499)

GoAhead Webserver information disclosure vulnerability VU#124059 (http://www.kb.cert.org/vuls/id/124059)

Rockwell Automation ControlLogix 1756-ENBT/A EtherNet/IP Bridge Knowledge base document:
http://rockwellautomation.custhelp.com/cgi-bin/rockwellautomation.cfg/php/enduser/std_adp.php?p_faqid=57729

Contact:

Doug Newbauer
Manager of Alerts
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-2009-02-13-01