Open Redirect Vulnerability MicroLogix, CompactLogix 5370 Controllers

Version 1.0 – April 23, 2019

Rockwell Automation received a report from ICS-CERT regarding an open redirect vulnerability in the web server of certain small Programmable Logic Controllers (PLCs) that, if successfully exploited, could allow a threat actor to inject arbitrary web content into the affected device's web pages. Affected product families include CompactLogix™ 5370 controllers and MicroLogix™ controllers.

Customers using affected versions of this firmware are encouraged to evaluate their risk and apply the appropriate mitigations provided below to their deployed products. Additional details relating to the discovered vulnerability, including affected products and recommended countermeasures, are provided herein.

AFFECTED PRODUCTS

MicroLogix 1400 Controllers
- Series B, v15.002 and earlier
- Series A, All Versions

MicroLogix 1100 Controllers
- v14.00 and earlier

CompactLogix 5370 L1 controllers
- v30.014 and earlier

CompactLogix 5370 L2 controllers
- v30.014 and earlier

CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix® controllers)
- V30.014 and earlier

VULNERABILITY DETAILS

These devices contain a web server that accepts user inputs via web interface. A remote, unauthenticated threat actor could utilize this function in conjunction with a social engineering attack to redirect the user from the affected controller's web server to a malicious website of the threat actor's choosing. This malicious website could potentially run or download arbitrary malware on the user's machine. The target of this type of attack is not the industrial control device and does not disrupt its control functionality.

CVE-2019-10955 has been assigned to this vulnerability. Rockwell Automation evaluated the vulnerability using the Common Vulnerability Scoring System ("CVSS") v3.0. A CVSS v3 base score of **7.1/10** has been assigned. For a better understanding of how this score was generated, please follow this link with the CVSS v3 vector string: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L.

RISK MITIGATIONS and RECOMMENDED USER ACTIONS

Customers are encouraged to assess their level of risk with respect to their specific applications and update to the latest available firmware revision that addresses the associated risk. Customers who are unable to update are directed to the risk mitigation strategies provided below and are encouraged, when possible, to combine these strategies with the general security guidelines to employ multiple strategies simultaneously.

Product	Catalog Numbers	Suggested Actions
MicroLogix 1400 controllers, Series A	1766-L32AWA 1766-L32AWAA 1766-L32BWA 1766-L32BWAA 1766-L32BXB 1766-L32BXBA	• No direct mitigation provided. • Affected users may disable the web server altogether by changing the HTTP setting from Enabled to Disabled using the LCD. See the 1766-UM001M-EN-P MicroLogix 1400 Programmable Controllers User Manual for more information
MicroLogix 1400 controllers, Series B	1766-L32AWA 1766-L32AWAA 1766-L32BWA 1766-L32BWAA 1766-L32BXB 1766-L32BXBA	• Apply FRN 15.003 or later for MicroLogix 1400 Series B devices (Download) • Affected users may disable the web server altogether by changing the HTTP setting from Enabled to Disabled using the LCD. See the 1766-UM001M-EN-P MicroLogix 1400 Programmable Controllers User Manual for more information
MicroLogix 1100 controllers	1763-L16BWA 1763-L16AWA 1763-L16BBB 1763-L16DWD	• Apply FRN 15.000 or later (Download) • Affected users may disable the web server altogether by

		unchecking the “HTTP Server Enable” checkbox in the Channel 1 configuration.
CompactLogix 5370 L1 controllers	1769-L16ER-BB1B 1769-L18ER-BB1B 1769-L18ERM-BB1B 1769-L19ER-BB1B	Apply v31.011 or later (Download)
CompactLogix 5370 L2 controllers	1769-L24ER-QB1B 1769-L24ER-QBFC1B 1769-L27ERM-QBFC1B	Apply v31.011 or later (Download)
CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix controllers)	1769-L30ER 1769-L30ER - NSE 1769-L30ERM 1769-L30ERMS 1769-L33ER 1769-L33ERM 1769-L33ERMS 1769-L36ERM 1769-L36ERMS 1769-L37ERMO 1769-L37ERMOS	Apply v31.011 or later (Download)

GENERAL SECURITY GUIDELINES

1. Use trusted software, software patches, anti-virus/anti-malware programs and interact only with trusted websites and attachments.
2. Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
3. Locate control system networks and devices behind firewalls and isolate them from the business network.
4. When remote access is required, use secure methods, such as virtual private networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. VPN is only as secure as the connected devices.
5. Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.

For further information on the Vulnerability Handling Process for Rockwell Automation, please refer to our Product Security Incident Response FAQ document.

Refer to our Industrial Network Architectures Page for comprehensive information about implementing validated architectures designed to complement security solutions.

Refer to the Network Services Overview Page for information on network and security services for Rockwell Automation to enable assessment, design, implementation and management of validated, secure network architectures.

We also recommend that concerned customers continue to monitor this advisory by subscribing to updates on the Security Advisory Index for Rockwell Automation, located at: 54102 - Industrial Security Advisory Index.

Rockwell Automation remains committed to making security enhancements to our systems in the future. For more information and for assistance with assessing the state of security of your existing control system, including improving your system-level security when using Rockwell Automation and other vendor controls products, you can visit the Rockwell Automation Security Solutions web site.

Requests for additional information can be sent to the RASecure Inbox (rasecure@ra.rockwell.com).
Please direct all media inquiries to Keith Lester (klester@ra.rockwell.com).

ADDITIONAL LINKS

- 54102 - Industrial Security Advisory Index
- Industrial Firewalls within a CPwE Architecture
- Deploying Industrial Firewalls within a CPwE Architecture Design and Implementation Guide
- [ICS-CERT/NCCIC] ICSA-19-113-01 Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers

REVISION HISTORY

Date	Version	Details
23-April-2019	1.0	Initial release

The most current version of this Industrial Security Advisory is posted on the Rockwell Automation Support Center, http://www.rockwellautomation.com/knowledgebase, as ID number 1086288.

DISCLAIMER

This document is intended to provide general technical information on a particular subject or subjects and is not an exhaustive treatment of such subjects. Accordingly, the information in this document is not intended to constitute application, design, software or other professional engineering advice or services. Before making any decision or taking any action, which might affect your equipment, you should consult a qualified professional advisor.

ROCKWELL AUTOMATION DOES NOT WARRANT THE COMPLETENESS, TIMELINESS OR ACCURACY OF ANY OF THE DATA CONTAINED IN THIS DOCUMENT AND MAY MAKE CHANGES THERETO AT ANY TIME IN ITS SOLE DISCRETION WITHOUT NOTICE. FURTHER, ALL INFORMATION CONVEYED HEREBY IS PROVIDED TO USERS "AS IS." IN NO EVENT SHALL ROCKWELL AUTOMATION BE LIABLE FOR ANY DAMAGES OF ANY KIND INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOST PROFIT OR DAMAGE, EVEN IF ROCKWELL AUTOMATION HAS BEEN ADVISED OFTHE POSSIBILITY OF SUCH DAMAGES.

ROCKWELL AUTOMATION DISCLAIMS ALL WARRANTIES WHETHER EXPRESSED OR IMPLIED IN RESPECT OF THE INFORMATION (INCLUDING SOFTWARE) PROVIDED HEREBY, INCLUDING THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, AND NON-INFRINGEMENT. NOTE THAT CERTAIN JURISDICTIONS DO NOT COUNTENANCE THE EXCLUSION OF IMPLIED WARRANTIES; THUS, THIS DISCLAIMER MAY NOT APPLY TO YOU