CompactLogix 5370 Programmable Automation Controllers Denial of Service Vulnerabilities

Version 1.0 – April 30, 2019

Rockwell Automation received two reports about potential vulnerabilities affecting versions of CompactLogix™ 5370 Programmable Automation Controllers. A successful exploitation of one of these potential vulnerabilities could result in a Denial of Service ("DoS") condition to the web portal of the affected device. A successful exploitation of the second vulnerability could potentially result in a DoS to the controller where it enters a major non-recoverable fault ("MNRF"). A MNRF is considered a safe state. Further details about MNRFs can be found in the vulnerability details section.

Customers using the affected products are strongly encouraged to evaluate the mitigations provided below and apply the appropriate mitigations to their deployed products. Additional details relating to the discovered vulnerability, including affected products and recommended security guidelines, are provided herein.

At the time of this writing, the Rockwell Automation® Product Security Incident Response Team ("PSIRT") is unaware of any active exploitation of these potential vulnerabilities.

AFFECTED PRODUCTS

- CompactLogix 5370 L1 controllers, versions 20 to 30.014 and earlier
- CompactLogix 5370 L2 controllers, versions 20 to 30.014 and earlier
- CompactLogix 5370 L3 controllers, versions 20 to 30.014 and earlier
- Compact GuardLogix® 5370 controllers, versions 20 to 30.014 and earlier
- Armor™ Compact GuardLogix 5370 controllers, versions 20 to 30.014 and earlier

VULNERABILITY DETAILS

About Major Non-Recoverable Faults ("MNRFs")

If a MNRF occurs in a CompactLogix controller, all I/O modules will transition to their configured fault state (for example Hold Last State). Memory will be marked as invalid and cleared. It is important to note that the memory clear is controlled and intentional, as the controller has determined internally that something is wrong and cannot guarantee continued safe controller execution. As a result, the controller goes into a Major Non-Recoverable Faulted state, which is considered safe. Recovery requires that you download the application program again.

Vulnerability #1: Email Object Stack Overflow Denial of Service

Rockwell Automation received a report describing a vulnerability where a remote, unauthenticated threat actor could send crafted SMTP configuration packets to port 44818 potentially causing a Denial of Service condition, where the controller enters a major non-recoverable faulted state (“MNRF”).

CVE-2019-10954 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 8.6/10 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:N/S:C/C:N/I:N/A:H

Vulnerability #2: Web Portal Denial of Service

Younes Dragoni of Nozomi Networks discovered a Denial of Service vulnerability in the web server of CompactLogix 5370 PLCs. By sending specific requests to the web server, a remote, unauthenticated threat actor could potentially force the web server to become unreachable, potentially preventing the user from gaining web access to view live controller data. A reset of the device is required to recover the web server. The control functions of the product are not affected by this vulnerability.

CVE-2019-10952 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 5.3/10 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:N/S:U/C:N/I:N/A:L

RISK MITIGATIONS and RECOMMENDED USER ACTIONS

1. Rockwell Automation strongly recommends that customers use the latest available version of firmware to keep up to date with the latest features, anomaly fixes, and security improvements. Update to a version of firmware as listed below that mitigates the associated risk:

Product Family	Actions	Notes
CompactLogix 5370	Apply FRN 31.011 or later	Download
Compact GuardLogix 5370	Apply FRN 31.011 or later	Download
Armor Compact GuardLogix 5370	Apply FRN 31.011 or later	Download

2. For EtherNet/IP™ based vulnerabilities, block all traffic to from outside the Manufacturing Zone by blocking or restricting access to TCP and UDP Port# 2222 and Port# 44818 using proper network infrastructure controls, such as firewalls, UTM devices, or other security appliances. For more information on TCP/UDP ports used by Rockwell Automation Products, see Knowledgebase Article ID 898270.

    a. Stratix® switch users can use Device Manager or Studio 5000 Logix Designer® software to configure access control lists (ACL) to block/restrict ports. See section “Access Control Lists” in Stratix Managed Switches User Manual, publication 1783-UM007, for detailed instructions.

3. Utilize proper network infrastructure controls, such as firewalls, to help ensure that SMTP packets from unauthorized sources are blocked.
4. Consult the product documentation for specific features, such as a hardware key-switch setting, to which may be used to block unauthorized changes, etc.
5. Use trusted software, software patches, antivirus/antimalware programs and interact only with trusted web sites and attachments.
6. Minimize network exposure for all control system devices and/or systems, and ensure that they are **not** accessible from the Internet. For further information about the risks of unprotected Internet accessible control systems, please see Knowledgebase Article ID 494865.
7. 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. Also recognize that VPN is only as secure as the connected devices.

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 (secure@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-19-120-01 Rockwell Automation CompactLogix 5370

REVISION HISTORY

Date	Version	Details
30-APR-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 1075979.