America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Rockwell Automation MicroLogix 1400 and CompactLogix 5370 Controllers

Last Revised: April 23, 2019 **Alert Code:** ICSA-19-113-01

1. EXECUTIVE SUMMARY

- **CVSS v3 7.1**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Rockwell Automation
- **Equipment:** MicroLogix 1400 and CompactLogix 5370 Controllers
- **Vulnerability:** Open Redirect

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to input a malicious link redirecting users to a malicious website.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Rockwell Automation products are affected:

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

3.2 VULNERABILITY OVERVIEW

3.2.1 URL REDIRECTION TO UNTRUSTED SITE ('OPEN REDIRECT') CWE-601 <https://cwe.mitre.org/data/definitions/601.html>

An open redirect vulnerability could allow a remote unauthenticated attacker to input a malicious link to redirect users to a malicious site that could run or download arbitrary malware on the user's machine.

CVE-2019-10955 has been assigned to this vulnerability. A CVSS v3 base score of 7.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:c/c:l/i:l/a:l>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

3.4 RESEARCHER

Josiah Bryan and Geancarlo Palavicini reported this vulnerability to NCCIC.

4. MITIGATIONS

Rockwell Automation has released a security advisory with mitigation steps that can be found at:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1086288 <https://rockwellautomation.custhelp.com/app/answers/detail/a_id/1086288> (Login required)

Rockwell Automation recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Update to the latest available firmware revision that addresses the associated risk.
- Use trusted software, software patches, anti-virus/anti-malware programs, and interact only with trusted websites and attachments.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and devices behind firewalls and isolate them from the business network.
- 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.
- Employ training and awareness programs to educate users on the warning signs of a phishing or social engineering attack.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website </ics/> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

NCCIC also recommends that users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams </reading_room/emailscams_0905.pdf> for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks </cas/tips/st04-014.html> for more information on social engineering attacks.

No known public exploits specifically target this vulnerability.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Rockwell Automation

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov