ICS Advisory (ICSA-22-090-05)

Rockwell Automation Logix Controllers

Legal Notice

All information products included in https://us-cert.cisa.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://us-cert.cisa.gov/tlp/.

1. EXECUTIVE SUMMARY

- **CVSS v3 10.0**
- **ATTENTION:** Exploitable remotely/low attack complexity
- **Vendor:** Rockwell Automation
- **Equipment:** Logix Controllers
- **Vulnerability:** Inclusion of Functionality from Untrusted Control Sphere

2. RISK EVALUATION

Successful exploitation of this vulnerability may allow an attacker to modify user programs. A user could then unknowingly download those modified elements containing malicious code.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Rockwell Automation reports the vulnerability affects the following products:

- 1768 CompactLogix controllers
- 1769 CompactLogix controllers

- CompactLogix 5370 controllers
- CompactLogix 5380 controllers
- CompactLogix 5480 controllers
- Compact GuardLogix 5370 controllers
- Compact GuardLogix 5380 controllers
- ControlLogix 5550 controllers
- ControlLogix 5560 controllers
- ControlLogix 5570 controllers
- ControlLogix 5580 controllers
- GuardLogix 5560 controllers
- GuardLogix 5570 controllers
- GuardLogix 5580 controllers
- FlexLogix 1794-L34 controllers
- DriveLogix 5730 controllers
- SoftLogix 5800 controllers

3.2 VULNERABILITY OVERVIEW

3.2.1 INCLUSION OF FUNCTIONALITY FROM UNTRUSTED CONTROL SPHERE CWE-829

An attacker with the ability to modify a user program may change user program code on some ControlLogix, CompactLogix, and GuardLogix Control systems. Studio 5000 Logix Designer writes user-readable program code to a separate location than the executed compiled code, allowing an attacker to change one and not the other.

CVE-2022-1161 has been assigned to this vulnerability. A CVSS v3 base score of 10.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

3.3 BACKGROUND

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

3.4 RESEARCHER

Sharon Brizinov and Tal Keren of Claroty reported this vulnerability to CISA.

4. MITIGATIONS

Users using the affected software or controllers are directed towards the risk mitigation steps listed below and are encouraged, when possible, to combine this guidance with the general security guidelines for a comprehensive defense-in-depth strategy.

The following mitigations should be applied for ControlLogix 5560, ControlLogix 5570, ControlLogix 5580 series, GuardLogix 5570, GuardLogix 5580, GuardLogix 5380, CompactLogix, CompactLogix 5380 devices:

Risk Mitigation A:

- Recompile and download user program code (i.e., acd).
- Put controller mode switch into Run position.

If keeping controller mode switch in Run is impractical, use the following mitigation:

- Recompile and download user program code (i.e., acd).
- Monitor controller change log for any unexpected modifications or anomalous activity.
- Utilize the Controller Log feature.
- Utilize Change Detection in the Logix Designer Application.
- If available, use the functionality in FactoryTalk AssetCenter software to detect changes.

Risk Mitigation B:

Implement CIP Security to help prevent unauthorized connections when properly deployed. Supported controllers and communications modules include:

- ControlLogix 5580 processors using on-board EtherNet/IP port.
- GuardLogix 5580 processors using on-board EtherNet/IP port.
- ControlLogix 5580 processors operating in High Availability (HA) configurations using 1756-EN4TR
- ControlLogix 5560, ControlLogix 5570, ControlLogix 5580, GuardLogix 5570 and GuardLogix 5580 can use a 1756-EN4TR ControlLogix EtherNet/IP module.
    - If using a 1756-EN2T, then replace with a 1756-EN4TR
- CompactLogix 5380 using on-board EtherNet/IP port.
- CompactLogix GuardLogix 5380 using on-board EtherNet/IP port.

The following mitigations should be applied for 1768 CompactLogix, 1769 CompactLogix, CompactLogix 5370, and CompactLogix 5480 devices:

- Recompile and download user program code (i.e., acd).
- Put controller mode switch into Run position.

If keeping controller mode switch in Run is impractical, then use the following mitigation:

- Recompile and download user program code (i.e., acd).
- Monitor controller change log for any unexpected modifications or anomalous activity.
- Use the Controller Log feature.
- Use Change Detection in the Logix Designer application.
- If available, use the functionality in FactoryTalk AssetCenter to detect changes.

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

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.

- Locate control system networks and remote 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

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

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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

No known public exploits specifically target this vulnerability.

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.