America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS ADVISORY

Rockwell Automation MicroLogix 1400 Controllers and 1756 ControlLogix Communications Modules

Last Revised: December 06, 2018 **Alert Code:** ICSA-18-310-02

1. EXECUTIVE SUMMARY

- **CVSS v3 8.6**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Rockwell Automation
- **Equipment:** MicroLogix 1400 Controllers and 1756 ControlLogix Communications Modules
- **Vulnerability:** Missing Authentication for Critical Function

2. REPOSTED INFORMATION

This advisory was originally posted to the HSIN ICS-CERT library on November 6, 2018, and is being released to the NCCIC/ICS-CERT website.

3. RISK EVALUATION

Successful exploitation of this vulnerability could allow an unauthenticated attacker to modify system settings and cause a loss of communication between the device and the system.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

Rockwell Automation reports the vulnerability affects the following PLC products:

MicroLogix 1400 Controllers

- Series A, all versions
- Series B, v21.003 and earlier
- Series C, v21.003 and earlier

1756 ControlLogix EtherNet/IP Communications Modules

- 1756-ENBT, all versions
- 1756-EWEB
  - Series A, all versions
  - Series B, all versions

- 1756-EN2F
  - Series A, all versions
  - Series B, all versions
  - Series C, v10.10 and earlier
- 1756-EN2T
  - Series A, all versions
  - Series B, all versions
  - Series C, all versions
  - Series D, v10.10 and earlier
- 1756-EN2TR
  - Series A, all versions
  - Series B, all versions
  - Series C, v10.10 and earlier
- 1756-EN3TR
  - Series A, all versions
  - Series B, v10.10 and earlier

4.2 VULNERABILITY OVERVIEW

4.2.1 MISSING AUTHENTICATION FOR CRITICAL FUNCTION CWE-306 <https://cwe.mitre.org/data/definitions/306.html>

An unauthenticated, remote threat actor could send a CIP connection request to an affected device, and upon successful connection, send a new IP configuration to the affected device even if the controller in the system is set to Hard RUN mode. When the affected device accepts this new IP configuration, a loss of communication occurs between the device and the rest of the system as the system traffic is still attempting to communicate with the device via the overwritten IP address.

CVE-2018-17924 has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:c/c:n/i:n/a:h>).

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing, Food and Agriculture, Transportation Systems, Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

4.4 RESEARCHER

David Noren reported this vulnerability to NCCIC.

5. MITIGATIONS

Rockwell Automation recommends users of affected products update to an available firmware revision that addresses the associated risk. Users who are unable to update their firmware are directed towards additional risk mitigation strategies provided herein and are encouraged to combine these with the general security guidelines to employ multiple strategies simultaneously, when possible.

Rockwell Automation suggests the following actions for affected versions:

- MicroLogix 1400 Controllers 1766-Lxxx, Series A, no direct mitigation provided. See additional mitigating recommendations below for suggested actions.
- For MicroLogix 1400 Controllers 1766-Lxxx, Series B or C, apply FRN 21.004 and later. Once the new FRN is applied, use the LCD Display to put the controller in RUN mode to prevent configuration changes. See p. 115 of the MicroLogix 1400 Programmable Controllers User Manual (1766-UM001M-EN-P) for details (available at the following location):

https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1766-um001_-en-p.pdf <https://literature.rockwellautomation.com/idc/groups/literature/documents/um/1766-um001_-en-p.pdf>

The download for FRN 21.004 can be found at the following location:

https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?Keyword=1766-L&crumb=112

- 1756 EtherNet/IP Web Server Module, 1756-EWEB, all series, no direct mitigation provided. See additional mitigating recommendations below for suggested actions.
- 1756 ControlLogix EtherNet/IP Communications Modules, 1756-ENBT, all versions, 1756-EN2F Series A, all versions, Series B, all versions. 1756-EN2T, Series A, all versions, Series B, all versions, Series C, all versions. 1756-EN2TR Series A, all versions, Series B, all versions. 1756-EN3TR Series A. No direct mitigation provided. See additional mitigating recommendations below for suggested actions.
- 1756 ControlLogix EtherNet/IP Communications Modules, 1756-EN2F, Series C, 1756-EN2T, Series D, 1756-EN2TR, Series C, 1756-EN3TR, Series B. The recommendations are to apply FRN 11.001 and later. Once the new FRN is applied, enable Explicit Protected Mode. See p. 32 of the EtherNet/IP Network Configuration User Manual (ENET-UM001-EN-P) for details. Available at the following location:

https://literature.rockwellautomation.com/idc/groups/literature/documents/um/enet-um001_-en-p.pdf <https://literature.rockwellautomation.com/idc/groups/literature/documents/um/enet-um001_-en-p.pdf>

The download for FRN 11.001 can be found at the following location:

https://compatibility.rockwellautomation.com/Pages/MultiProductDownload.aspx?Keyword=1756-EN&crumb=112

Rockwell Automation suggests the following additional mitigating recommendations for affected versions:

- Utilize proper network infrastructure controls, such as firewalls, to help ensure that EtherNet/IP messages from unauthorized sources are blocked.
- Consult the product documentation for specific features, such as a hardware key switch setting, which may be used to block unauthorized changes, etc.
- Block all traffic to EtherNet/IP or other CIP protocol-based devices from outside the operational zone by blocking or restricting access to Port 2222/TCP and UDP 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.
- Use trusted software, software patches, antivirus/antimalware 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.

For additional information, Rockwell Automation recommends users continue to monitor their advisory by subscribing to updates on the Security Advisory Index for Rockwell Automation, located at: 54102 - Industrial Security Advisory Index at the following location (login required):

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102

<https://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102>

NCCIC 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 that they are not accessible from the Internet </ics/alerts/ics-alert-10-301-01>.
- 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 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.

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.

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

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>