2025

AutoTableTop™ Scenario based on Rockwell Advisory PN1633

Robert Rhodes

Derezzed Inc. D/B/A ThreatGEN

1/24/2025

Rockwell Product Security Scenario

For ThreatGEN AutoTableTop™ (as requested by Rockwell)

Contents

Summary

This scenario is an example of a tabletop exercise scenario simulating an openly posted advisory PN1633[1] that could be used as the basis for an automated tabletop exercise within AutoTableTop™. This scenario is based solely on publicly available information regarding the vulnerability in Rockwell Automation's FactoryTalk Service Platform. It does not include any non-public information about the CVE or any specific outcomes related to its exploitation. The purpose of this scenario is to provide a realistic framework for organizations to test and improve their incident response capabilities in a controlled environment.

A nation-state actor has developed and exploited a critical vulnerability in Rockwell Automation's FactoryTalk Linx product. The vulnerability allows remote code execution without authentication, potentially compromising industrial control systems. A security researcher has discovered and reported this vulnerability to Rockwell Automation's product security team.

We've tackled this scenario from the **perspective of the equipment provider;** future scenarios from ThreatGEN may include these three likely industrial users perspectives.

About the Equipment Provider

Rockwell Automation is a global leader in industrial automation and digital transformation, headquartered in Milwaukee, Wisconsin. Founded in 1903, the company has grown to employ approximately 27,000 people and serves customers in more than 100 countries worldwide. Rockwell Automation's business is structured around three primary segments: Intelligent Devices, Software & Control, and Lifecycle Services.

The company's product portfolio includes the Allen-Bradley brand of automated components and integrated control systems, which are widely used in various industries for safety, sensing, and control applications. The Software & Control segment offers a comprehensive suite of production automation and operations platforms, including both hardware and software solutions. **This segment is particularly relevant to the recent vulnerability, as it encompasses the FactoryTalk software suite, which includes FactoryTalk Linx and the FactoryTalk Service Platform.**

FactoryTalk Linx is a critical component of Rockwell Automation's software offerings, serving as the primary communications platform for The Connected Enterprise. It facilitates real-time data exchange between various Allen-Bradley control hardware and software systems, enabling seamless integration of IT and OT environments. The FactoryTalk Service Platform, which includes FactoryTalk

[1] https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1633.html

Linx, is a foundational element present in most Rockwell Automation software products, providing essential services such as data access, system management, and security features.

The vulnerability in question, CVE-2024-21915, affects the FactoryTalk Service Platform (FTSP). This security flaw is classified as an "*Incorrect Execution-Assigned Permissions*" vulnerability, which could allow a malicious user with basic privileges to escalate their access to administrator-level permissions within the FTSP. The potential impact of this vulnerability is significant, as it could enable unauthorized users to read, modify, or delete sensitive data, and potentially render the FTSP system unavailable.

Summary of the vulnerability

CVE-2024-21915 is a privilege escalation vulnerability in Rockwell Automation's FactoryTalk Service Platform versions prior to v2.74. If exploited, an attacker with basic user group privileges could potentially sign into the software and receive FTSP Administrator Group privileges. This could lead to unauthorized access to sensitive data, data modification, deletion, and potential system unavailability. The vulnerability has been assigned a CVSS v3.1 base score of 9.0, indicating its critical nature.

Rockwell Automation has advised customers to apply available patches and implement security best practices to mitigate the risk. The company also recommends that users minimize network exposure for control system devices, ensure they are not directly accessible from the internet, and use secure methods like VPNs for remote access when necessary.

References

1) Rockwell Automation Company Profile:
https://www.rockwellautomation.com/en-us/company/about-us.html

2) FactoryTalk Linx Information:
https://www.rockwellautomation.com/en-us/products/software/factorytalk/operationsuite/communications/linx.html

3) CVE-2024-21915 Advisory:
https://www.cisa.gov/news-events/ics-advisories/icsa-24-046-16

4) Rockwell Automation Business Segments:
https://investors.rockwellautomation.com/company-information/business-segments/default.aspx

5) FactoryTalk Service Platform Overview:
https://www.rockwellautomation.com/en-us/capabilities/industrial-automation-control/design-and-configuration-software.html

Industrial Users of Affected Equipment

The Rockwell Automation FactoryTalk Service Platform (FTSP) vulnerability (CVE-2024-21915) poses a significant threat to industrial environments across multiple sectors. In these scenarios, the privilege escalation vulnerability in FTSP could allow attackers with basic access to gain administrator-level control, potentially leading to severe operational, safety, and economic consequences. The critical nature of these industries makes them attractive targets for both state-sponsored actors and cybercriminals seeking to cause disruption or extort organizations[2].

Organizations in these sectors must prioritize patching this vulnerability and implement additional security measures such as network segmentation, multi-factor authentication, and continuous monitoring to mitigate the risk of exploitation.

Oil and Gas Industry

In the oil and gas sector, FTSP is likely used to manage and control critical processes in refineries and pipeline operations. The vulnerability could allow attackers to:

- Manipulate refinery control systems, potentially altering production parameters
- Interfere with pipeline monitoring and control, risking environmental disasters
- Access sensitive operational data, including production volumes and schedules

For example, an attacker could exploit this vulnerability to gain unauthorized access to a major pipeline's control systems, like the Colonial Pipeline incident, potentially disrupting fuel distribution across large regions[3].

Manufacturing Industry

In manufacturing, FTSP is crucial for automating production lines and managing factory operations. Exploitation of this vulnerability could lead to:

- Unauthorized changes to production recipes or parameters
- Disruption of just-in-time inventory systems
- Theft of proprietary manufacturing processes

[2] https://ogma.in/mitigating-cve-2024-21915-rockwell-automation-factorytalk-service-platform-privilege-escalation-vulnerability
[3] https://multivistaglobal.com/safety-first-how-rockwells-automation-solutions-help-reduce-industrial-hazards/

A real-world scenario might involve an attacker gaining admin privileges in an automotive manufacturing plant, allowing them to alter robotic assembly line parameters, potentially causing production of defective vehicles or halting production entirely[4].

Power Generation and Distribution

The power sector relies heavily on industrial control systems for grid management and power plant operations. The FTSP vulnerability in this context could enable:

- Unauthorized control of power generation equipment
- Manipulation of grid distribution systems
- Access to critical infrastructure data

An attacker exploiting this vulnerability could potentially gain control over a power plant's SCADA systems, allowing them to disrupt power generation or distribution, causing widespread blackouts[5].

[4] https://ultech-engineering.com/rockwellautomations-cybersecurity-solutions/
[5] https://www.cisa.gov/news-events/ics-advisories/icsa-24-046-16

AutoTableTop™ Settings – Rockwell Perspective

This scenario will test Rockwell Automation's ability to respond to a critical product security incident, balancing the need for thorough analysis and patch development with timely customer communication and public disclosure.

Threat Scenario

A nation-state actor has developed and exploited a critical vulnerability in Rockwell Automation's FactoryTalk Linx product. The vulnerability allows remote code execution without authentication, potentially compromising industrial control systems. A security researcher has discovered and reported this vulnerability to Rockwell Automation's product security team.

Company

Rockwell Automation

Company information

Rockwell Automation is a global leader in industrial automation and digital transformation. The company provides solutions for various industries, including manufacturing, process control, and critical infrastructure. Rockwell's products and services include control systems, industrial control software, and IoT-enabled devices.

Department

The exercise will focus on the following departments:

- Product Security Team
- Software Development Team
- Public Relations/Communications
- Legal Department
- Executive Leadership

Exercise Objectives

1) Test the product security incident response plan for a critical vulnerability.
2) Evaluate the communication process between the product security team and software development team.
3) Assess the decision-making process for developing and releasing a security patch.
4) Practice crafting and disseminating a security advisory to customers and the public.
5) Evaluate the coordination between technical teams and PR/Legal departments in managing the incident's public disclosure.

Participants

- Chief Product Security Officer
- Lead Software Developer
- Public Relations Director

- Legal Counsel
- Chief Technology Officer

Cybersecurity Staff

- Product Security Manager
- Vulnerability Assessment Specialist
- Security Patch Development Lead
- Threat Intelligence Analyst
- Security Advisory Coordinator

Leadership Staff

- CEO
- CTO
- CISO
- VP of Software Development
- VP of Customer Relations

Network Environment

The scenario focuses on Rockwell's internal development and testing environment for FactoryTalk Linx, including:

1) Source code repositories
2) Build and testing servers
3) Vulnerability assessment tools
4) Internal communication systems
5) Customer support portals

Injects

1) A security researcher reports a critical vulnerability in FactoryTalk Linx to Rockwell's product security team.
2) Initial analysis confirms the vulnerability's severity and potential for remote code execution.
3) Evidence suggests a nation-state actor has already exploited the vulnerability in the wild.
4) The development team identifies challenges in creating a patch without disrupting customer operations.
5) A major customer inquires about rumors of a security flaw in FactoryTalk Linx.
6) Legal team raises concerns about potential liability issues related to the vulnerability.
7) A cybersecurity news outlet reaches out for comment on the alleged vulnerability.
8) The patch development process encounters unexpected delays.
9) Internal debate arises over the appropriate timeline for public disclosure.
10) Executive leadership requests a briefing on the potential business impact of the vulnerability.

Attachment - Rockwell Advisory PN1633

PN1633 | Remote Code Execution and Denial-of-Service Vulnerabilities in Select Communication Modules

Severity:

High

Advisory ID:

PN1633

Published Date:

July 12, 2023

Last Updated:

July 12, 2023

Revision Number:

1.0

Known Exploited Vulnerability (KEV):

No

Corrected:

No

Workaround:

No

CVE IDs

CVE-2023-3596,

CVE-2023-3595

Summary

Remote Code Execution and Denial-of-Service Vulnerabilities in Select Communication Modules

Revision History

Revision Number

1.0

Revision History

Version 1.0 – July 12, 2023

Executive Summary

Rockwell Automation, in coordination with the U.S. government, has analyzed a novel exploit capability attributed to Advance Persistent Threat (APT) actors affecting select communication modules. We are not aware of current exploitation leveraging this capability, and intended victimization remains unclear. Previous threat actors cyberactivity involving industrial systems suggests a high likelihood that these capabilities were developed with an intent to target critical infrastructure and that victim scope could include international customers. Threat activity is subject to change and customers using affected products could face serious risk if exposed.

Rockwell Automation has provided patches for all affected products, including hardware series that were out of support. Detection rules have also been provided.

Exploitation of these vulnerabilities could allow malicious actors to gain remote access of the running memory of the module and perform malicious activity, such as manipulating the module's firmware, inserting new functionality into the module, wiping the module's memory, falsifying traffic to/from the module, establishing persistence on the module, and potentially affect the underlying industrial process. This could result in destructive actions where vulnerable modules are installed, including critical infrastructure.

Customers using the affected products are strongly encouraged to evaluate and implement the mitigations provided below. Additional details relating to the discovered vulnerabilities, including the products in scope, impact, and recommended countermeasures, are provided below.

Affected Products

Catalog	Series	Versions
1756-EN2T 1756-EN2TK 1756-EN2TXT	A,B,C	<=5.008 & 5.028
	D	<=11.003
1756-EN2TP 1756-EN2TPK 1756-EN2TPXT	A	<=11.003
1756-EN2TR 1756-EN2TRK 1756-EN2TRXT	A, B	<=5.008 & 5.028
	C	<=11.003
1756-EN2F 1756-EN2FK	A, B	<=5.008 & 5.028
	C	<=11.003
1756-EN3TR 1756-EN3TRK	A	<=5.008 & 5.028
	B	<=11.003
1756-EN4TR 1756-EN4TRK 1756-EN4TRXT	A	<=5.001

Vulnerability Details

CVE-2023-3595
Where this vulnerability exists in the 1756 EN2* and 1756 EN3* products, it could allow a malicious user to perform remote code execution with persistence on the target system through maliciously crafted CIP messages. This includes the ability to modify, deny, and exfiltrate data passing through the device.

CVSS score: 9.8/10 (Critical)
CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE-787: Out-of-bounds Write

CVE-2023-3596
Where this vulnerability exists in the 1756-EN4* products, it could allow a malicious user to cause a denial of service by asserting the target system through maliciously crafted CIP messages.

CVSS Score: 7.5/10 (High)
CVSS vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE-787: Out-of-bounds Write

Risk Mitigation & User Action

These vulnerabilities can be addressed by performing a standard firmware update. Customers are strongly encouraged to implement the risk mitigations provided below and to the extent possible, to combine these with the QA43240 - Recommended Security Guidelines from Rockwell Automation to employ multiple strategies simultaneously.

Catalog	Series	Affected Versions	Remediations
1756-EN2T 1756-EN2TK 1756-EN2TXT	A,B,C	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	D	<=11.003	Update to 11.004 or later
1756-EN2TP 1756-EN2TPK 1756-EN2TPXT	A	<=11.003	Update to 11.004 or later

1756-EN2TR 1756-EN2TRK 1756-EN2TRXT	A, B	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	C	<=11.003	Update to 11.004 or later
1756-EN2F 1756-EN2FK	A, B	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	C	<=11.003	Update to 11.004 or later
1756-EN3TR 1756-EN3TRK	A	<=5.008 & 5.028	• Update to 5.029 or later for signed versions (**recommended). • Update to 5.009 for unsigned versions.
	B	<=11.003	Update to 11.004 or later
1756-EN4TR 1756-EN4TRK 1756-EN4TRXT	A	<=5.001	Update to 5.002 or later

** Rockwell Automation strongly recommends updating to signed firmware if possible. Once the module is updated to signed firmware (example 5.008 to 5.029), it is not possible to revert to unsigned firmware versions.

Mitigations

Organizations should take the following actions to further secure ControlLogix communications modules from exploitation.

- **Update firmware.** Update EN2* ControlLogix communications modules to firmware revision 11.004 and update EN4* ControlLogix communications modules to firmware revision 5.002.
- **Properly segment networks.** Given a cyber actor would require network connectivity to the communication module to exploit the vulnerability, organizations should ensure ICS/SCADA networks are properly segmented within the process structure as well as from the Internet and other non-essential networks.
- **Implement detection signatures.** Use appended Snort signatures to monitor and detect anomalous Common Industrial Protocol (CIP) packets to Rockwell Automation devices.

Additionally, organizations should increase protections of ICS/SCADA networks by implementing at least the following mitigations:

- Regularly back up devices to allow for reversion to a clean copy of firmware or a working project;
- disable unused CIP objects on communications modules, such as unused CIP Email and Socket Objects;
- block all traffic to CIP-enabled devices from outside the ICS/SCADA network using available security products; and
- monitor CIP traffic for unexpected content or unusual packets lengths.

Potential Indicators of Compromise

System owners should ensure ICS/SCADA networks are baselined and regularly monitored for deviations in network activity. Specifically, systems owners can look for the following potential IOCs (Indicators of Compromise) for ControlLogix communications modules:

- Unknown scanning on a network for Common Industrial Protocol (CIP)-enabled devices.
- Unexpected or out-of-specification CIP packets to CIP objects implemented in ControlLogix communications modules, including the Email Object and non-public vendor-specified objects.
- Arbitrary writes to communication module memory or firmware.
- Unexpected firmware updates.
- Unexpected disabling of secure boot options.

- Uncommon firmware file names.

Detection Rules

The following Snort rules are intended to be run on a computer with network visibility of a ControlLogix communications module and can be used to detect traffic to a ControlLogix communications module that does not conform to the CIP specification as provided by ODVA (Open DeviceNet Vendors Association). While both the CIP Email and Socket Objects are capable of communicating over a network, they are intended to communicate over the backplane of a ControlLogix PLC (Programmable Logic Controller) and therefore should not be seen over the network. However, it is possible that site engineers could configure a communications module such that there is legitimate network traffic to and from CIP Email and Socket Objects, potentially resulting in false positives.

Snort 2 Rules and Snort 3 Rules are both attached below.

References

- CVE-2023-3595 JSON
- CVE-2023-3596 JSON

Attachments

File

CVE-2023-3595 Snort 2.rules

Attachments

File

CVE-2023-3595 Snort 3.rules