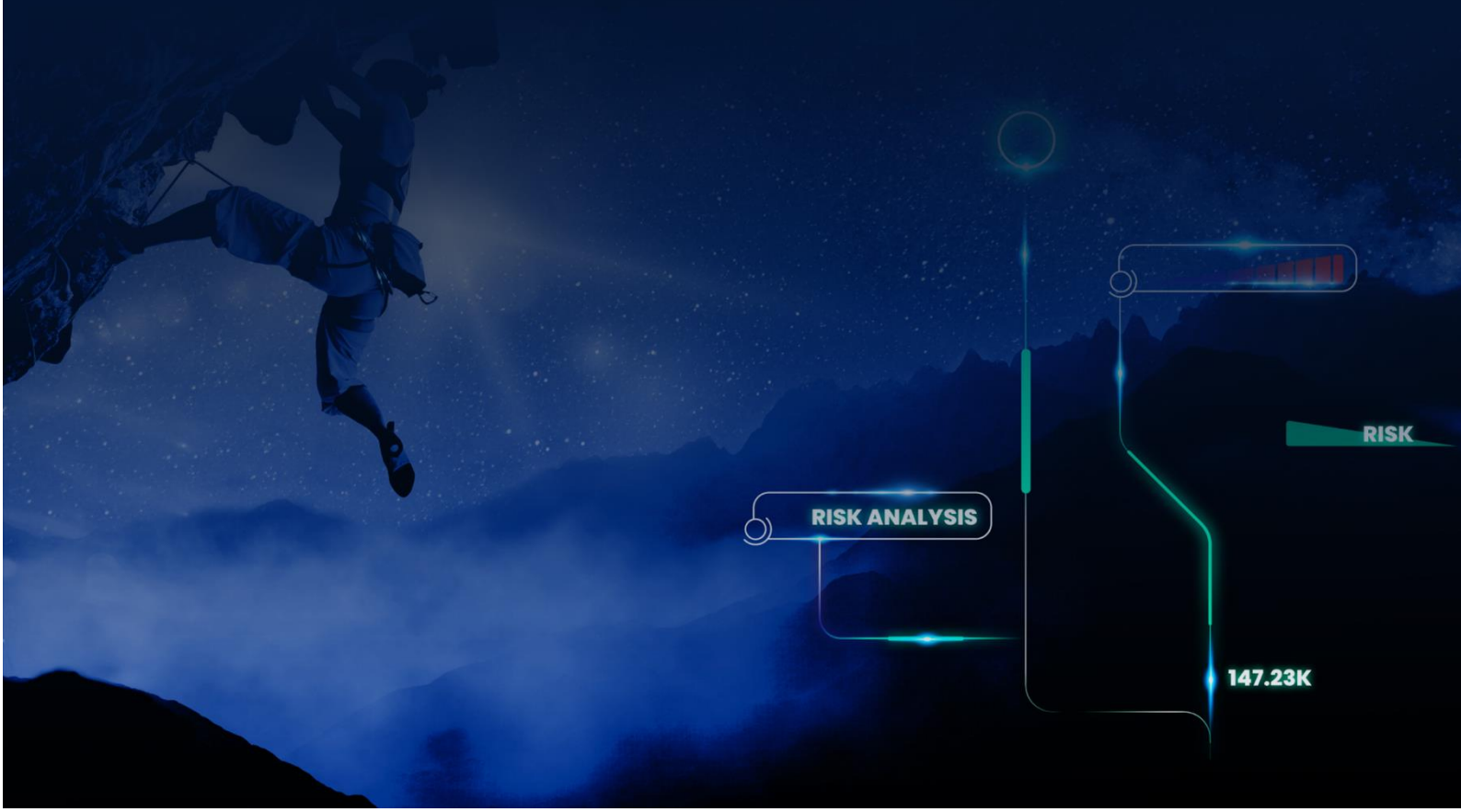
Radiflow

Advisory: Rockwell and Honeywell Critical Vulnerabilities

July 17th 2023



Executive Summary

Rockwell Automation's and Honeywell each released a security advisory regarding critical vulnerabilities in automation systems. Rockwell Automation published on July 12 that the ControlLogix communication modules, particularly the 1756-EN2*,1756-EN3*, and 1756-EN4* series, were identified as having high-risk vulnerabilities, with a CVSS v3 score of 9.8. These vulnerabilities could allow remote access to the module's running memory, potentially enabling malicious activities. According to Rockwell, these vulnerabilities were attributed to an unnamed Advanced Persistent Threat (APT) group, although they are not currently aware of any exploitation leveraging these vulnerabilities.

The following day, Honeywell published an advisory highlighting a series of similarly high-severity (CVSS 9.8) vulnerabilities in the Experion PKS, LX, and PlantCruise platforms. The risks, including buffer overflows and uncontrolled resource consumption, could lead to denial of service, privilege escalation, or remote code execution.

The purpose of this brief is to advise Radiflow customers and partners using its iSID industrial threat detection system how to detect various Indicators of Compromise (IOCs) of these critical vulnerabilities. Customers and partners are advised to update the Snort rules package in the iSID to the latest version "SNORT_2023_07_16".

Radiflow

Technical Analysis

These recently disclosed vulnerabilities in Rockwell and Honeywell's industrial control systems present a potential threat causing remote code execution or denial of service.

Rockwell

Rockwell has identified 2 new vulnerabilities in the ControlLogix communication modules.

- **CVE-2023-3595 (CVSS 9.8)** - A critical out-of-bounds writing vulnerability. A malicious actor could exploit this by sending a specially crafted Common Industrial Protocol (CIP) message that is larger than expected, resulting in data being written beyond its intended boundaries. This vulnerability affects 1756 EN2* and 1756 EN3* products, potentially allowing remote code execution.
- **CVE-2023-3596 (CVSS 7.5)** - A high-severity out-of-bounds writing vulnerability. A malicious actor could exploit this by sending a specially crafted Common Industrial Protocol (CIP) message that is larger than expected, resulting in data being written beyond its intended boundaries. This vulnerability affects the 1756 EN4* products and could lead to a denial of service (DoS).

Honeywell

Honeywell has identified 9 new vulnerabilities in the Experion PKS, LX, and PlantCruise systems. 7 of the 9 vulnerabilities are critical with a CVSS score of 9.8 and 2 have a High severity CVSS score of 7.5.

- **CVE-2023-25078 (9.8)** - A Stack-based buffer overflow vulnerability. A malicious actor could exploit this vulnerability by sending a specially crafted message to an unnamed specific configuration operation, causing a memory buffer overflow. This can allow the attacker remote code execution (RCE) or lead to a denial of service (DoS).
- **CVE-2023-23585 (9.8) and CVE-2023-24474 (9.8)** - Heap-based buffer overflow vulnerabilities. A malicious actor could exploit them by sending a specially crafted message to an unnamed specific configuration operation, causing a memory buffer overflow. This can lead to a denial of service (DoS).
- **CVE-2023-25948 (9.8)** - A malicious actor could exploit this vulnerability by sending a specially crafted message that promotes the Experion C300 module to return an error message leaking system configuration data.
- **CVE-2023-24480 (9.8)**, **CVE-2023-25435 (9.8)**, **CVE-2023-25770 (9.8), and CVE-2023-26597 (7.5)** - Buffer and stack overflow vulnerabilities caused by mishandling of system data. A malicious actor can send a crafted message exploiting the system flaw and cause a denial of service (DoS).
- **CVE-2023-25178 (7.5)** Due to insufficient authentication a malicious actor can upload malicious firmware which could enable remote code execution.

CVE	CVSS Score	Affected Products
CVE-2023-3595	9.8	Rockwell ControlLogix EtherNet/IP models, 1756-EN2*, 1756-EN3*
CVE-2023-3596	7.5	Rockwell ControlLogix EtherNet/IP model 1756-EN4
CVE-2023-23585	9.8	Honeywell Experion Server or Console Station
CVE-2023-25078	9.8	
CVE-2023-25948	9.8	Honeywell Experion C300
CVE-2023-26597	7.5	
CVE-2023-24480	9.8	
CVE-2023-25770	9.8	
CVE-2023-25178	7.5	
CVE-2023-22435	9.8	Honeywell Experion Server
CVE-2023-24474	9.8	

Radiflow

Detection by iSID

iSID is equipped with powerful monitoring engines, specifically designed to detect any attempts at exploiting the vulnerabilities. The system enables you to devise custom rules and alerts, enhancing your defensive capabilities by monitoring for potential signs of exploitation.

Network visibility

Network visibility actively monitors connections between devices within the network.
Utilize this engine to create the following alerts:

1. **Internet-Connected Networks**

Rule Name	Rule Patterns/additional information
IP address in your network suspected to be in the internet	The attacker will initiate the connection with the target
New link detected	With the above mentioned internet IP address
New protocol detected	Look for ENIP CIP communication TCP port 44818 and UDP 2222 related to the external IP
New protocol detected	Look for Honeywell communication on the following ports TCP/55550 from the external IP

2. **Internal Networks**

Rule Name	Rule Patterns/additional information
New link detected	From an unexpected internal address
New protocol detected	Look for ENIP CIP communication TCP port 44818 and UDP 2222 related to an unexpected internal address
New protocol detected	Look for Honeywell communication on the following ports TCP/55550 from unexpected internal address

Cyber Attack Rules

Cyber Attack Rules engine actively monitors network traffic to detect malicious activity based on pre-defined SNORT rules.
Activate the following recommended SNORT rules to detect exploitation of the recent Rockwell vulnerabilities.

- PROTOCOL-SCADA ENIP CIP Socket Object unconnected read with unusual length
- PROTOCOL-SCADA ENIP CIP Socket Object unconnected ucmm read with unusual length
- PROTOCOL-SCADA ENIP CIP Socket Object connected read with unusual length
- PROTOCOL-SCADA ENIP CIP Socket Object connected ucmm read with unusual length

- PROTOCOL-SCADA ENIP CIP Vendor Specific Object unconnected parameter 1 contains unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object unconnected parameter 2 contains unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object unconnected ucmm parameter 1 contains unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object unconnected ucmm parameter 2 with unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object connected parameter 1 contains unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object connected parameter 2 with unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object connected ucmm parameter 1 contains unusual length
- PROTOCOL-SCADA ENIP CIP Vendor Specific Object connected ucmm parameter 2 contains unusual length

The following SNORT rules may be triggered during an attempt to exploit the Rockwell vulnerabilities.

- PROTOCOL-SCADA Rockwell firmware upload attempt
- PROTOCOL-SCADA Rockwell Controllogix Network Policy Change attempt
- PROTOCOL-SCADA Rockwell Controllogix Stop CPU attempt
- PROTOCOL-SCADA Rockwell Controllogix Dump Boot Code attempt
- PROTOCOL-SCADA Rockwell Controllogix Ethernet Reset attempt
- PROTOCOL-SCADA Rockwell Controllogix Crash CPU attempt
- PROTOCOL-SCADA Rockwell Controllogix Crash Ethernet attempt
- SERVER-OTHER Rockwell Automation RSLinux heap buffer overflow attempt
- PROTOCOL-SCADA Real-time Automation Ethernet/IP buffer overflow attempt
- PROTOCOL-SCADA Rockwell Automation RSLinx Classic buffer overflow attempt
- ROCKWELL Automation ControlLogix Denial of Service (CPU Stop)
- ROCKWELL Automation ControlLogix Denial of Service (Crash CPU)
- ROCKWELL Automation ControlLogix EtherNET/IP modules boot code dump (Dump)

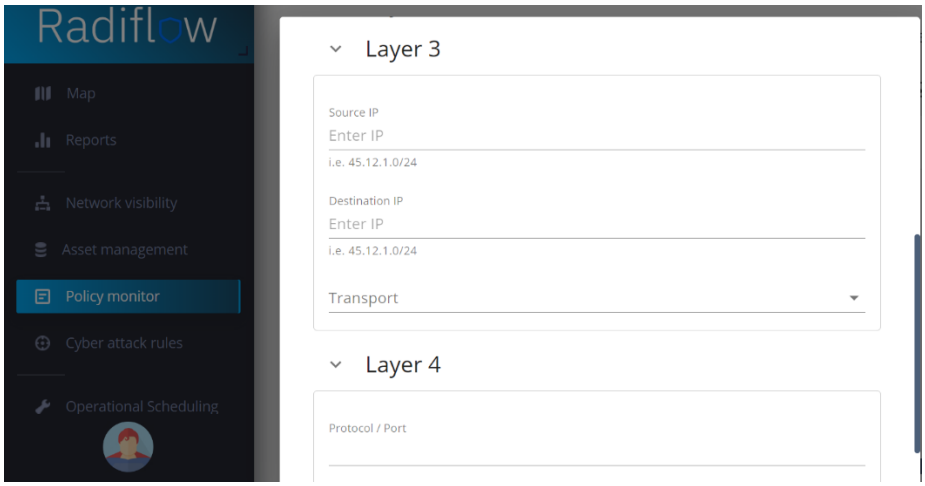
Radiflow

Policy Monitor

Policy Monitor engine actively monitors network traffic to detect malicious activity based on a set of rules. The engine generates rule suggestions based on observed network traffic, and manual rule creation is also possible.

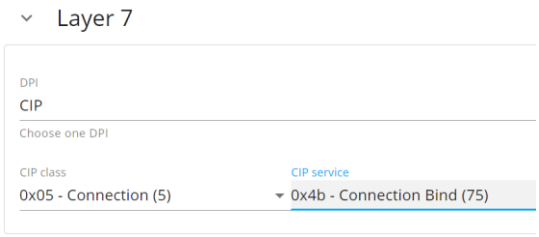
Honeywell

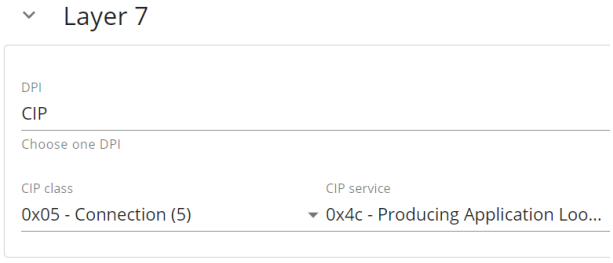
To detect unusual activity or unauthorized communication indicative of exploit attempts of the Honeywell vulnerabilities add a rule tracking new communication from unexpected assets to an affected asset using Honeywell ports TCP/55550.



Rockwell

To detect unusual activity or unauthorized communication indicative of exploit attempts of the Rockwell vulnerabilities add rules tracking new communication from unexpected assets to an affected asset using the following layer 7 configurations.





Mitigations

Vendors Firmware/Software Update

Vendors official advisories are attached to this advisory. Use the following table to update the affected products to their mitigated versions:

Vendor	Product	Mitigated version
Rockwell	1756-EN4TR Series A	5.002 or later
Rockwell	1756-EN4TRK Series A	
Rockwell	1756-EN4TRXT Series A	
Rockwell	1756-EN2F Series A, B	5.029 or later for signed versions and 5.009 for unsigned versions
Rockwell	1756-EN2FK Series A, B	
Rockwell	1756-EN2TK Series A, B, C	
Rockwell	1756-EN2T Series A, B, C	
Rockwell	1756-EN2TXT Series A, B, C	
Rockwell	1756-EN2TR Series A, B	
Rockwell	1756-EN2TRK Series A, B	
Rockwell	1756-EN2TRXT Series A, B	
Rockwell	1756-EN3TR Series A	
Rockwell	1756-EN3TRK Series A	
Rockwell	1756-EN2TP Series A	11.004 or later
Rockwell	1756-EN2TPK Series A	
Rockwell	1756-EN2TPXT Series A	
Rockwell	1756-EN2TR Series C	
Rockwell	1756-EN2TRK Series C	
Rockwell	1756-EN2TRXT Series C	
Rockwell	1756-EN2TXT Series D	
Rockwell	1756-EN2TK Series D	
Rockwell	1756-EN2T Series D	
Rockwell	1756-EN3TR Series B	
Rockwell	1756-EN3TRK Series B	
Honeywell	Experion PKS	R520.2
Honeywell	Experion LS	
Honeywell	Experion PlantCruise	

Network Segmentation

Properly segmenting the ICS/SCADA networks and disconnecting them from the Internet can help prevent the attacker from establishing a connection to the affected asset.

Hardening - block vulnerable services

Rockwell

- 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

Honeywell

- If embedded chart monitoring is not required - block port 55550
- If there are clients that require embedded chart monitoring for operations then access to port 55550 should be limited to only those clients.

Radiflow's additional recommendation:

- Audit remote connections to supervisory/operations/basic control zones based on approved protocols and workstations.
- Ensure basic cyber-hygiene practices:
  - Enforce multifactor authentication for remote access to ICS networks and devices
  - Regularly change all passwords of ICS/SCADA devices and systems, especially default passwords, to strong per-device passwords.
  - Regularly back up devices.

If you suspect malicious ICS network activity, or for additional guidance, you are welcome to reach out to the Radiflow cyber analytics team.

Sources and additional info

https://www.cisa.gov/news-events/ics-advisories/icsa-23-194-06

https://process.honeywell.com/ and search for "SN2023-06-22".

https://www.cisa.gov/news-events/ics-advisories/icsa-23-193-01

https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140010

https://www.tenable.com/blog/cve-2023-3595-cve-2023-3596-rockwell-automation-controllogix-vulnerabilities-disclosed