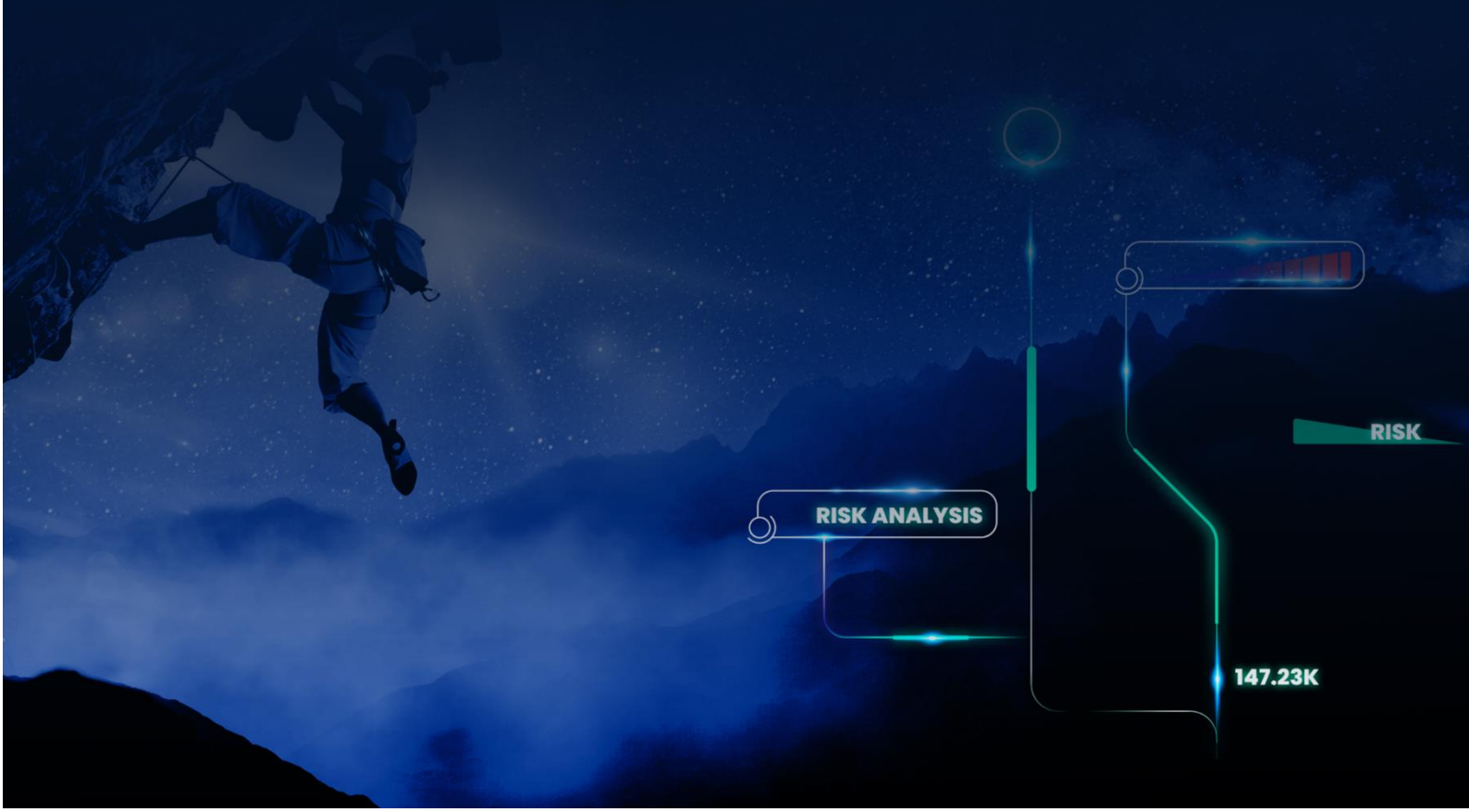
Radiflow

Advisory: Rockwell, CODESYS, OPTO 22 and KNX Vulnerabilities

September 06, 2023



Executive Summary

The recent ICS advisories issued by CISA on August 24, 2023, highlight vulnerabilities in industrial automation and control systems from Rockwell Automation, CODESYS, and OPTO 22, and in devices using the KNX protocol. These vulnerabilities include a range of cybersecurity threats, from Out-of-Bounds Write to Uncontrolled Search Path Element and Improper Access Control issues, each with its own set of potential consequences, including remote exploitation and denial-of-service attacks.

ICSA ID	CVE	CVSS	Affected Product
ICSA-23-236-01	CVE-2023-4346	7.5	devices using the KNX Protocol
ICSA-23-236-02	CVE-2023-40706	7.5	OPTO 22 SNAP PAC S1
	CVE-2023-40707	7.5	
	CVE-2023-40708	5.3	
	CVE-2023-40709	5.9	
	CVE-2023-40710	5.9	
ICSA-23-236-03	CVE-2023-3662	7.3	CODESYS Development System: versions from 3.5.17.0 and prior to 3.5.19.20
ICSA-23-236-04	CVE-2023-3669	3.3	CODESYS Development System: versions prior to 3.5.19.20
ICSA-23-236-05	CVE-2023-3663	9.6	CODESYS Development System: versions from 3.5.11.0 and prior to 3.5.19.20
ICSA-23-236-06	CVE-2022-1737	8.6	Rockwell Automation Input/Output Modules

Radiflow

Technical Analysis

CVE-2023-4346 (7.5)

A vulnerability affecting the availability and control of KNX devices has been identified. This vulnerability occurs when using a direct IP connection to connect KNX devices. Devices can connect with either KNX connection Secure enabled or disabled. Devices where KNX connection Secure is disabled lack a security password, also known as a BCU Key. A malicious actor could exploit this vulnerability by connecting to the device without needing a password. Once connected, they could change the device's configuration and establish a new password/BCU Key, effectively locking out authorized users. To modify the device configuration or reset the password, the current password is required, making recovery impossible.

Detection

Radiflow customers and partners can use the iSID Network Visibility detection engine to detect suspicious connections to the KNX devices.

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 previous internet IP adders
New link detected	From an unexpected internal address
New protocol detected	Look for KNX communication on TCP port 3671 and UDP 2222 related to the external IP or an unexpected internal IP address

CVE-2023-40706 (7.5)

This vulnerability is caused by SNAP PAC S1 not having limits on the number of login attempts to the built-in web server. This could allow a malicious actor to perform a brute-force attack and gain access to the built-in web server.

CVE-2023-40707 (7.5)

This vulnerability is caused by SNAP PAC S1 not requiring a complex password. This could allow a malicious actor to perform a successful brute force attack if users don't set complex credentials.

CVE-2023-40708 (5.3)

An improper access control vulnerability in SNAP PAC S1, caused by The File Transfer Protocol (FTP) port being open by default. This could allow a malicious actor to access device files.

CVE-2023-40709 (5.9)

This vulnerability is caused when the SNAP PAC S1 controller has the built-in web server enabled, but not completely set up and configured. A malicious actor could cause the controller to crash by sending a large quantity of ICMP requests.

CVE-2023-40710 (5.9)

This vulnerability is caused when the SNAP PAC S1 controller has the built-in web server enabled, but not completely set up and configured. A malicious actor could cause the controller to crash by sending a large quantity of HTTP GET requests.

CVE-2023-3662 (7.3)

This vulnerability in CODESYS Development System versions allows unauthorized users to execute binary files from the program's current working directory. This could lead to unauthorized code execution, data tampering, or compromise of the user's system.

CVE-2023-3669 (3.3)

This vulnerability is caused by the CODESYS Development System not having limits on the number of password attempts. This could allow a malicious actor to perform a brute-force attack and gain access.

CVE-2023-3663 (9.6)

This vulnerability is caused by the CODESYS Development System not having an integrity check for notifications received by the CODESYS notification server. This could allow a malicious actor to manipulate the content of notifications received via HTTP.

CVE-2023-1737 (8.6)

An out-of-bounds write vulnerability in Pyramid Solutions' Developer and DLL kits for EtherNet/IP Adapter and EtherNet/IP Scanner affects select Input/Output Modules from Rockwell Automation. A malicious actor can send a specially crafted packet to cause a denial of service on the affected products.

Mitigations

CVE-2023-4346 (7.5)

The KNX Association recommends the following steps for mitigating devices using the KNX Protocol.

- Set a strong BCU Key on KNX devices

CVE-2023-40706, CVE-2023-40707, CVE-2023-40708, CVE-2023-40709, CVE-2023-40710

OPTO 22 recommends the following steps for mitigating the SNAP PAC S1 controller.

- Disable the built-in web server when not in use through the Network Security settings within the OPTO 22 Pac Manager software.
- Restrict access to the built-in web server found on HTTPS (TCP/443).
- Restrict access to the FTP Port (TCP/21).
- Ensure user credentials are changed to something long, complex, and unique.

CVE-2023-3662, CVE-2023-3669, CVE-2023-3663

CODESYS and CISA recommend the following steps for mitigating the CODESYS Development System.

- Update the CODESYS Development System to version 3.5.19.20.
- Exercise principles of least privilege.

CVE-2022-1737 (8.6)

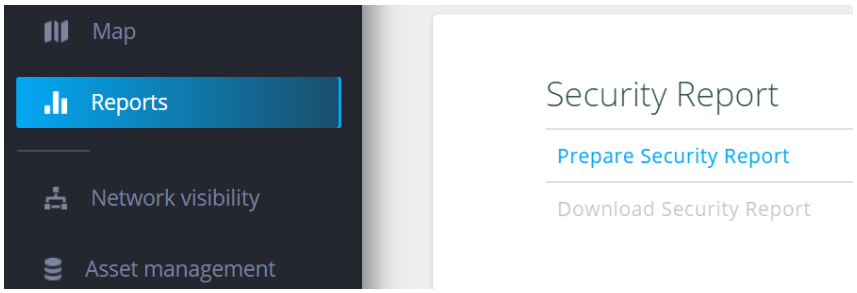
Rockwell Automation recommends the following steps for mitigating the affected Input/Output Modules.

- Update the Input/Output Module to the mitigated version (see table below).

Radiflow

Visibility

Radiflow customers and partners using iSID can create a security report and check if they are using affected Rockwell I/O modules with the affected versions.



In addition, Radiflow customers and partners can use Radiflow Active Scan to scan the Rockwell I/O modules and get their version to check if they are using an affected version of the Rockwell I/O module.

Affected Product	Affected Version	Mitigated Version
1734-AENT/1734-AENTR Series C	7.011 and prior	7.013
1734-AENT/1734-AENTR Series B	5.019 and prior	5.021
1738-AENT/ 1738-AENTR Series B	6.011 and prior	6.013
1794-AENTR Series A	2.011 and prior	2.012
1732E-16CFGM12QCWR Series A	3.011 and prior	3.012
1732E-12X4M12QCDR Series A	3.011 and prior	3.012
1732E-16CFGM12QCR Series A	3.011 and prior	3.012
1732E-16CFGM12P5QCR Series A	3.011 and prior	3.012
1732E-12X4M12P5QCDR Series A	3.011 and prior	3.012
1732E-16CFGM12P5QCWR Series B	3.011 and prior	3.012
1732E-IB16M12R Series B	3.011 and prior	3.012
1732E-OB16M12R Series B	3.011 and prior	3.012
1732E-16CFGM12R Series B	3.011 and prior	3.012
1732E-IB16M12DR Series B	3.011 and prior	3.012
1732E-OB16M12DR Series B	3.011 and prior	3.012
1732E-8X8M12DR Series B	3.011 and prior	3.012
1799ER-IQ10XOQ10 Series B	3.011 and prior	3.012

Radiflow's additional recommendations:

- Properly segment the ICS/SCADA networks and make sure they are disconnected from the internet.
- 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 contact the Radiflow cyber analytics team.

Additional Info

https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-01
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-03
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-04
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-05
https://www.cisa.gov/news-events/ics-advisories/icsa-23-236-06
https://www.codesys.com/security/security-reports.html
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1140532