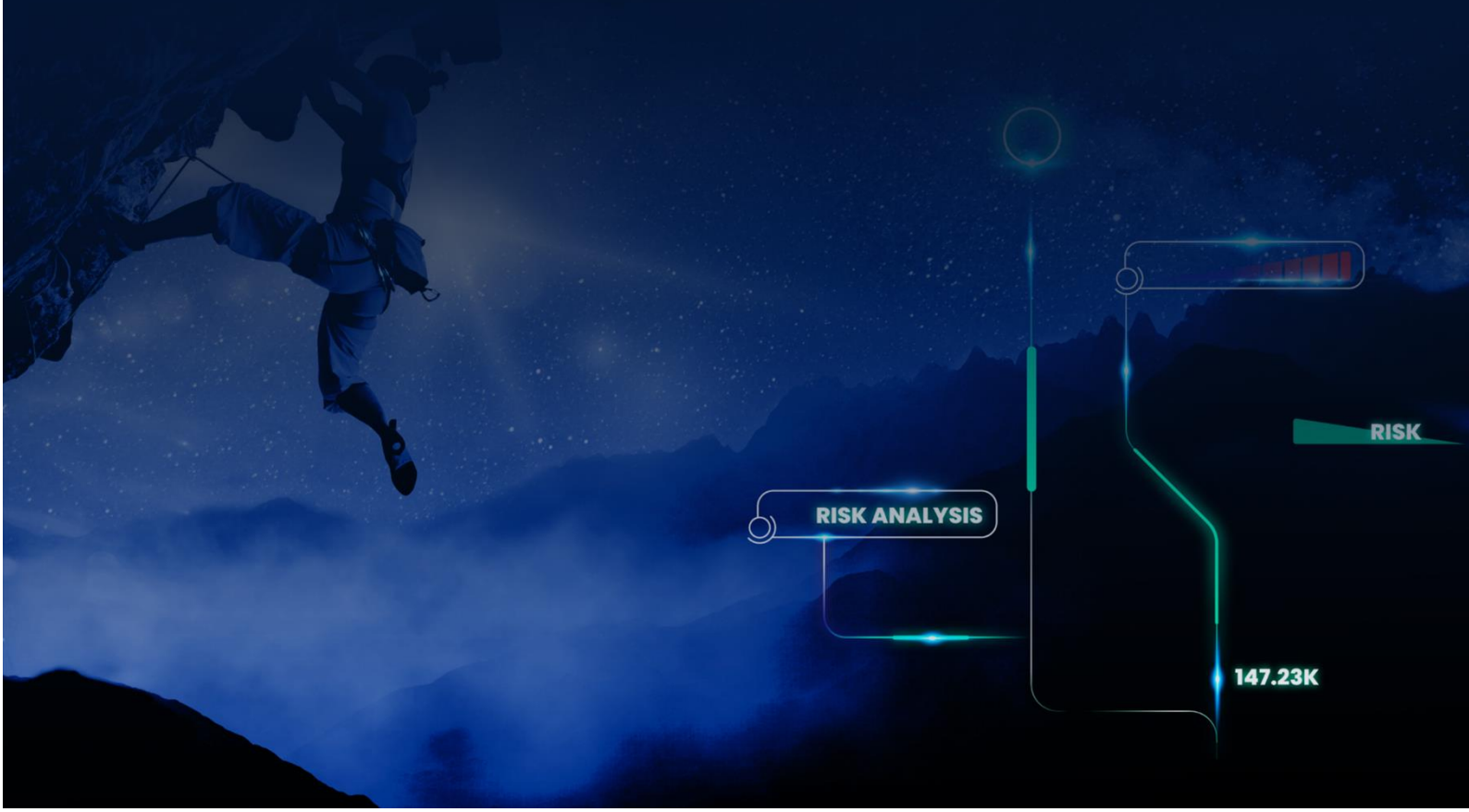
Radiflow

Quarterly ICS Security Report
2023 Q4



Radiflow

Contents

Executive Summary

This quarterly report offers a comprehensive analysis of noteworthy ICS cybersecurity incidents and published vulnerabilities from the fourth quarter of 2023. Our main goal is to provide Radiflow customers with up-to-date information on the latest cybersecurity incidents and newly identified critical and relevant vulnerabilities.

In this advisory, we highlight cybersecurity incidents occurring in various OT operators worldwide, along with vulnerabilities found in industrial automation and control systems from major manufacturers. Radiflow strongly recommends that its customers and partners review the vulnerabilities and implement necessary measures to mitigate them.

Notable ICS Cybersecurity Incidents

Water and Wastewater

- In early December, the Cyber Av3ngers group targeted a water system in a remote county in Ireland, resulting in a two-day disruption of water supply for the residents. They managed to breach the security of the Unitronics PLC by exploiting CVE-2023-6448 through default administrative passwords.
- Additionally, the group attempted an attack on the Municipal Water Authority of Aliquippa, US, although it did not lead to any water service interruptions. More information on the vulnerability and relevant mitigations below.
- The Paris Wastewater Agency, also known as SIAAP, experienced a cyber-attack of unknown origin in November. The agency promptly took measures to secure its industrial systems and prevent the attack from spreading. Additionally, they implemented measures to ensure the continuity of public sanitation services.

Power

- Slovenian power company Holding Slovenske Elektrarne (HSE) fell victim to a ransomware attack in November. This resulted in compromised systems and encrypted files, though power production remained unaffected. The attack is believed to be the work of the Rhysida ransomware gang.
- The Rhysida ransomware group executed a ransomware attack against the China Energy Engineering Corporation (CEEC), a state-owned energy company in China late November. Rhysida asserted that they had exposed "exclusive, unique, and substantial" data from CEEC.

Iron Swords – Israel War VS Hamas

During the war between Israel and Hamas, there were several cyber attacks aimed at OT and IoT devices and networks, here are some of the notable incidents.

BMS

- An unidentified malicious actor managed to gain access to a building management systems interface in large office buildings in Israel. This unauthorized access

occurred because the management interface had been left exposed to the Internet with a default password. The attacker proceeded to manipulate the building's electrical systems, toggling lights on and off, activating water boilers, and even shutting down the cooling system in the electric transformer room, nearly resulting in a potential fire hazard.

- Two distinct, unverified reports surfaced regarding unauthorized access to heating systems in medical facilities in Israel. On November 30, an individual claimed to have breached the heating system at “Dorot” Medical Center. On December 20, reports indicated an attack on the “ADI” Disability Care Center, where the attacker successfully accessed the heating system.

Oil&Gas

- A malicious actor executed an attack on gas stations across Iran on December 18th. The Iranian Minister of Oil confirmed that this attack had widespread consequences, impacting approximately 70% of the country's gas stations, and pointed fingers at Israel and the USA. At the same time, an Israeli hacker group known as "Predatory Sparrow" claimed responsibility for the attack. This incident occurred in parallel with Israeli reports accusing Iran and Hezbollah of an attack on the “ZIV” Hospital in northern Israel.

IOT

- Both the Israeli National Cyber Directorate and the Lebanese group Hezbollah have issued alerts about cyberattacks targeting private-owned security cameras, with the objective of gathering visual intelligence (VISINT) on military positions and operations. To protect these cameras from such attacks, the Israeli Government has issued an emergency regulation, granting authorization to the IDF and the Shin Bet to access and operate the computers responsible for controlling stationary cameras in Israel.

ICS Vulnerabilities

In this section of the cyber update, we offer an aggregated overview and statistics of cyber vulnerabilities and notable ICS vulnerabilities Published in Q4 of 2023.

Total new vulnerabilities in Q4: **7,779**

ICS vulnerabilities among these: **643**

Severity	# of CVEs
Critical	111
High	308
Medium	193
Low	31

Total new CISA KEVs (Known Exploited Vulnerabilities) in Q4 of 2023: **47**
ICS vulnerabilities among these: **6**

CVE	CVSS	Vendor	Product
CVE-2023-49897	8.8	FXC	AE1021, AE1021PE

CVE-2023-47565	8.8	QNAP	VioStor NVR
CVE-2023-6448	9.8	Unitronics	Vision Series, Samba Series
CVE-2023-4911	7.8	Siemens	SIMATIC S7-1500
CVE-2023-4863	8.8	Siemens	Mendix Studio Pro 7, 8, 9, 10.
CVE-2023-20198	10.0	Rockwell Automation	Stratix 5800 and Stratix 5200

CISA ICS Advisories

Notable advisories:

ICSA ID	CVE	CVSS	Affected Product
ICSA-23-348-15	CVE-2023-6448	9.8	Unitronics Vision
ICSA-23-320-13	CVE-2022-23218	9.8	Siemens SIMATIC MV500
	CVE-2022-23219	9.8	
ICSA-23-320-09	CVE-2020-25020	9.8	Siemens Comos
	CVE-2023-46601	9.6	
	CVE-2023-43505	9.6	
	CVE-2023-43504	9.6	
ICSA-23-320-01	CVE-2023-42770	10	Red Lion Sixnet RTUs
	CVE-2023-40151	10	
ICSA-23-306-06	CVE-2023-5402	9.8	Schneider Electric SpaceLogic C-Bus Toolkit
	CVE-2023-5399	9.8	
ICSA-23-297-01	CVE-2023-20198	10	Rockwell Automation Stratix 5800/5200
ICSA-23-290-01	CVE-2023-5391	9.8	Schneider Electric EcoStruxure Power Monitoring and Power Operation
ICSA-23-285-09	CVE-2023-36380	9.8	Siemens SICAM A8000 CPCI85 Firmware
ICSA-23-285-02	CVE-2023-22779	9.8	Siemens SCALANCE W1750D
	CVE-2023-22780	9.8	
	CVE-2023-22781	9.8	
	CVE-2023-22782	9.8	
	CVE-2023-22783	9.8	
	CVE-2023-22784	9.8	
	CVE-2023-22785	9.8	
	CVE-2023-22786	9.8	
ICSA-23-278-01	CVE-2022-22822	9.8	Hitachi Energy AFS65x, AFF66x, AFS67x, and AFR67x Series Products
	CVE-2022-22823	9.8	
	CVE-2022-22824	9.8	
	CVE-2022-25315	9.8	
	CVE-2022-25235	9.8	
	CVE-2022-25236	9.8	
	CVE-2022-23852	9.8	

Unitronics

CVE-2023- 6448 (9.8)

Unitronics VisiLogic (versions before 9.9.00) uses default administrative passwords. An unauthenticated attacker with network access to a PLC or HMI can take administrative control of the system.

Discovery

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

Rule Name	Rule Patterns/additional information
IP address in your network suspected to be in the internet	
New link detected	With the previous internet IP address
New protocol detected	Monitor Unitronics communication on TCP port 20256 from external IP

Mitigation

- Disconnect the PLC from the open internet.
- Update to version 9.9.00 or later version.
- Change all default passwords on PLCs.
- Use an allowlist of IPs for access.
- If possible, utilize a TCP port that is different than the default port TCP 20256.

Siemens

CVE-2022-23218 & CVE-2022-23219 (9.8)

Siemens Simatic MV500 (versions before V3.3.5) contains GNU C Library (aka glibc) which is vulnerable to a buffer overflow vulnerability potentially resulting in a denial of service or arbitrary code execution.

Mitigation

Update to V3.3.5 or a later version.

CVE-2022-25020 (9.8)

Siemens Comos contains the MPXJ component which is vulnerable to an Improper Restriction vulnerability potentially resulting in external entity injection (XXE).

Mitigation

Update Comos to V10.4.4 or a later version.

CVE-2023-46601 (9.6)

Siemens Comos lacks proper access controls in making the SQLServer connection. potentially allowing bypass of the access control and data infiltration.

Mitigation
Update Comos to V10.4.4 or a later version.

CVE-2023-43505 (9.6)

Siemens Comos lacks proper access controls in SMB shares potentially allowing bypass of the access control and data infiltration.
Mitigation

- Update Comos to V10.4.4 or a later version.
- Use an application server which builds an additional layer of access control.

CVE-2023-43504 (9.6)

Siemens Comos uses a service testing executable that is vulnerable to a buffer overflow vulnerability potentially resulting in a denial of service or arbitrary code execution.

Mitigation

- Update Comos to V10.4.4 or a later version.
- Delete ptmcast.exe from the bin folder of the COMOS installation directory.

CVE-2023-36380 (9.8)

Siemens SICAM A8000 CPCI85 Firmware contains a hard-coded SSH ID, allowing an attacker to login to the device via SSH.
Mitigation

- Update to CPCI85 V05.11 or a later version.

CVE-2023-22779, CVE-2023-22780, CVE-2023-22781, CVE-2023-22782, CVE-2023-22783, CVE-2023-22784, CVE-2023-22785, CVE-2023-22786 (9.8)

Siemens SCALANCE W1750D is vulnerable to 8 different buffer overflow vulnerabilities. Since SCALANCE W1750D doesn’t check the size of the input, a malicious actor can send specially crafted packets to the PAPI (Aruba's access point management protocol) UDP port 8211 causing a buffer overflow and executing arbitrary code as a privileged user.

Discovery
Radiflow customers and partners can use the iSID Network Visibility detection engine to detect suspicious connections to the SCALANCE W1750D devices.

Rule Name	Rule Patterns/additional information
IP address in your network suspected to be in the internet	
New link detected	With the previous internet IP address
New protocol detected	Monitor SCALANCE W1750D communication on UDP port 8211 from external IP

Mitigation

- Update to version V8.10.0.6 or later version.
- Use an allowlist of IPs for access.
- Block access to port UDP/8211 from untrusted networks.

Red Lion

CVE-2023-42770, CVE-2023-40151 (10.0)

Red Lion Sixnet RTUs are vulnerable to an authentication bypass vulnerability. When the RTU receives a message over TCP/IP instead of UDP/IP the RTU will simply accept the message with no authentication challenge.

Mitigation

- Red Lion released patches to block all Sixnet UDR messages over TCP/IP.

Schneider Electric

CVE-2023-5402, CVE-2023-5399 (9.8)

Schneider Electric's SpaceLogic C-Bus Toolkit contains a path traversal vulnerability allowing access to files on the PC running C-Bus. The Toolkit also has an improper privilege management vulnerability. These vulnerabilities could lead to remote code execution and unauthorized file tampering.

Discovery

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

Rule Name	Rule Patterns/additional information
IP address in your network suspected to be in the internet	
New link detected	With the previous internet IP address
New protocol detected	Monitor SpaceLogic communication on TCP port 20023 from external IP

Mitigation

- Update to version v1.16.4 or later version.
- Use an allowlist of IPs for access.
- Block access to port TCP/20023 from untrusted networks.

CVE-2023-5391 (9.8)

Schneider Electric's EcoStruxure Power Monitoring and Power Operation doesn't validate the source of the data before deserializing it. This allows an attacker to send malicious data packets that may lead to the execution of arbitrary code.

Mitigation

Schneider Electric has released A Hotfix for these vulnerabilities, Contact Schneider Electric's Customer Care Center.

Rockwell Automation

CVE-2023-20198 (10.0)
Rockwell Automation Stratix 5800 and 5200 use the web user interface feature of Cisco IOS XE. This interface is vulnerable, when exposed to the internet or untrusted networks it allows a remote, unauthenticated threat actor to create an account with high-privilege access.
Discovery
Radiflow customers and partners can use the iSID detection engines “Network Visibility” and “Cyber Attack Rules” to detect suspicious connections to the Stratix devices. The following “Network Visibility” rules may be triggered during an attack:

- IP address in your network suspected to be in the internet
- New link detected (from external IP)

The following SNORT signatures may be triggered during an attack: 3:62541 - SERVER-WEBAPP Cisco IOS XE Web UI authentication bypass attempt 3:62542 - SERVER-WEBAPP Cisco IOS XE Web UI authentication bypass attempt

Mitigation

- Disconnect Stratix devices from the internet.
- Follow the vendor instructions to disable the HTTP Server feature
- Use an allowlist of IPs for access.

Hitachi Energy

CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-25315, CVE-2022-25235, CVE-2022-25236, CVE-2022-23852(9.8)

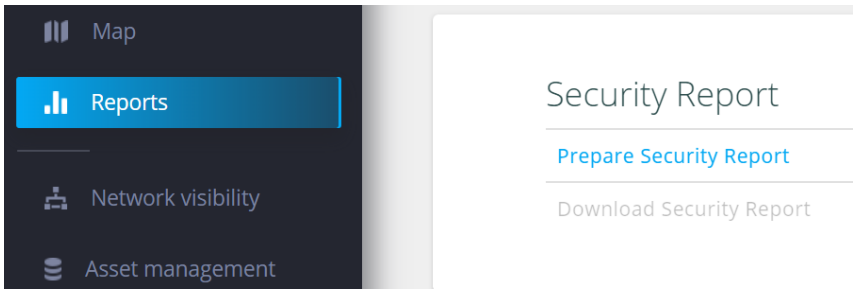
The following Hitachi Energy products contain the libexpat open-source library. This library in versions before 2.4.3 contains vulnerable code that can be exploited by a malicious actor.
The affected products:
AFF66X FW, AFS66X-S: All versions, AFS660-C: All versions, AFS66X-B: All versions, AFS670-V20: All versions, AFS65X: All versions, AFS67X: All versions, AFR677: All versions

Mitigation

Affected Devices	Mitigations
AFF66X FW 03.0.02 and earlier	update to upcoming AFF66X 04.x.xx FW when released.
AFS66X-S, AFS660-C, AFS66X-B, AFS670-V20	update to upcoming AFS66X, AFS670-V20 7.1.08 FW when released.
	Disable HTTP/HTTPS server or restrict access to HTTP/HTTPS to trusted IP addresses
	Disable IEC61850-MMS server or restrict access to IEC61850-MMS to trusted IP addresses.
AFS65X, AFS67X, AFR677	update to AFS65X, AFS67X, AFR677 09.1.08 FW.
	Disable HTTP/HTTPS server or restrict access to HTTP/HTTPS to trusted IP addresses.
	Disable IEC61850-MMS server

Visibility

Radiflow customers and partners using iSID can create a security report and check if they are using the affected products with the affected versions.



In addition, Radiflow customers and partners can use Radiflow Active Scan to scan the affected products and get their version to check if they are using an affected version of the products.

Radiflow's additional best practice 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.

Radiflow

CIARA Threat Intelligence Updates

We added 3 new threat groups to CIARA and updated 7 existing groups.

Threat groups added

Redfly

Symantec discovered a newly identified espionage group, Redfly, focused on Asia's critical national infrastructure (CNI). Redfly compromised an Asian national grid using the ShadowPad Trojan for six months

Sandman

Sentinel One observed a new threat actor named Sandman targeting telecom providers in the Middle East, Western Europe, and South Asia. Sandman deploys a unique backdoor called LuaDream based on the LuaJIT platform.

Snatch

CISA has released an advisory as part of an ongoing operation to #StopRansomware. The Snatch ransomware group is known for targeting critical sectors, employing tactics like data exfiltration and double extortion threats.

Threat groups updated

Following recent activities, the following threat group profiles and techniques were updated:

Threat Group	Techniques	Industry	Country	Region	Aliases
OilRig	V	V	V	V	X
Tonto Team	V	X	V	X	V
LockBit	V	X	X	X	X
APT28	V	V	V	V	V
DarkHydrus	V	X	X	X	V
MuddyWater	V	X	X	X	V
Ke3chang	V	X	V	X	V

To obtain the CIARA update files, kindly reach out to Radiflow Support.

Ongoing Support

Thank you for trusting Radiflow to reduce risks in your OT environment. We are committed to providing you with the latest insights and product improvements to defend against evolving threats.

If you suspect malicious ICS network activity, or for detailed information and support, please reach out to our team at support@radiflow.com or visit our official website at Radiflow.com.

Additional Info

https://downloads.unitronicsplc.com/Sites/plc/Visilogic/Version_Changes-Bug_Reports/VisiLogic%209.9.00%20Version%20changes.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-348-15
https://www.cisa.gov/news-events/ics-advisories/icsa-23-320-13
https://www.cisa.gov/news-events/ics-advisories/icsa-23-320-09
https://www.cisa.gov/news-events/ics-advisories/icsa-23-285-09
https://www.cisa.gov/news-events/ics-advisories/icsa-23-285-02
https://www.cisa.gov/news-events/ics-advisories/icsa-23-320-01
https://support.redlion.net/hc/en-us/articles/19338927539981-SixTRAK-and-VersaTRAK-Security-Patch-RLCSIM-2023-05
https://www.cisa.gov/news-events/ics-advisories/icsa-23-306-06
https://www.cisa.gov/news-events/ics-advisories/icsa-23-290-01
https://www.se.com/us/en/work/support/contacts.jsp
https://www.cisa.gov/news-events/ics-advisories/icsa-23-297-01
https://www.rockwellautomation.com/en-in/support/advisory.PN1653.html
https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/
https://www.cisa.gov/news-events/ics-advisories/icsa-23-278-01
https://publisher.hitachienergy.com/preview?DocumentId=8DBD000165&DocumentRevisionId=B&languageCode=en&Preview=true