Radiflow

Quarterly ICS Security Report
2024 Q3

Radiflow

Contents

Radiflow

Executive Summary

This quarterly report offers a comprehensive analysis of noteworthy ICS cybersecurity incidents and published vulnerabilities from the thread quarter of 2024. 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.

ICS Cybersecurity Incidents

Manufacturing

Schlatter Group, a Swiss manufacturer, was hit by a ransomware attack on August 9, 2024, which caused a 10-day disruption to its IT systems. The company revealed that malware was used, though details on the attack remain limited, and the identity of the attackers is still unknown. The breach impacted communications, including email systems, and caused delays in key projects.

Microchip Technology, a leading semiconductor and embedded control solutions provider, experienced a cyberattack that disrupted manufacturing and production across multiple facilities. The breach forced the company to shut down some systems and isolate affected ones to contain the impact, which hindered its ability to fulfill orders. Later, the ransomware group Play claimed responsibility for the attack.

Bassett Furniture, one of the largest U.S. furniture companies, shut down its production lines following a ransomware attack on July 10, 2024. The company detected unauthorized access that led to the encryption of various servers, forcing a shutdown of its IT systems to contain the breach. As a result, manufacturing operations were also halted. So far, no ransomware group has claimed responsibility for the attack.

Australian gold mining company Evolution Mining suffered a ransomware attack in August 2024, impacting its IT systems. While the company took steps to contain the breach, it confirmed both operational disruptions and a data breach.

Fresnillo PLC, the world's leading silver producer, suffered a cyberattack in July 2024, impacting its IT systems and leading to unauthorized access to data. Upon discovering the breach, Fresnillo initiated response measures to contain the attack. Fortunately, the attack

did not affect their OT (Operational Technology) systems, which continued to operate normally.

Energy

Halliburton, a major U.S. oil services company, was hit by a cyberattack on August 21, 2024, linked to the RansomHub ransomware gang. The attack disrupted its IT systems, forcing the company to take certain systems offline to contain the breach.

The ransomware group Handala has claimed responsibility for a cyberattack on BLEnergy, an Israeli energy company involved in energy storage. The attackers released 145 GB of sensitive data, alleging the motivation behind the attack was BLEnergy's collaboration with the IDF.

Water and Wastewater

Hackers targeted a water treatment plant in Arkansas City, compromising its systems and prompting a federal investigation. The breach raised concerns about potential risks to critical infrastructure, though no disruptions to water services were reported

Transportation

Seattle-Tacoma International Airport suffered a ransomware attack on August 24, 2024, by the Rhysida hacker group. The attack disrupted airport operations, forcing manual check-ins and affecting ground operations systems, such as baggage handling and flight displays. During the attack, Rhysida stole sensitive data and demanded a ransom of $6 million in Bitcoin, but the airport refused to pay.

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 Q3 of 2024.
Total new vulnerabilities in Q3: **8,560**
ICS vulnerabilities Published in Q3: **303**

severity	CVEs
Critical	32
High	148
Medium	115
Low	8

Total new CISA KEVs (Known Exploited Vulnerabilities) in Q3 of 2024: **59**
ICS Vulnerabilities Within CISA KEV: **0**

CISA ICS Advisories

Total new CISA ICS advisories in Q3 of 2024: **123**.
Notable ICS Vulnerabilities:

mySCADA

Product	CVE	CVSS	details	Mitigation
myPRO	CVE-2024-4708	9.8	Hard-coded password	Update to v8.31.0

Rockwell Automation

Product	CVE	CVSS	details	Mitigation
ThinManager ThinServer	CVE-2024-5988	9.8	The product doesn't validate the input from user allowing remote code execution	Update to the corrected software versions Limit remote access for TCP Port 2033
	CVE-2024-5989	9.8		
	CVE-2024-7988	9.8		
AADvance Standalone OPC-DA Server	CVE-2018-1285	9.8	A vulnerability in the log4net config file used by this product	Update to v2.02
DataMosaix Private Cloud	CVE-2024-6078	9.1	An improper authentication vulnerability allowing control of a legitimate user	Update to V7.09

Radiflow

SIEMENS

Product	CVE	CVSS	details	Mitigation
Industrial Edge Management	CVE-2024-45032	10.0	Improper validation of device tokens leading to authorization bypass	Update IEM Pro to V1.9.5 and IEM Virtual to V2.3.1-1
SINEMA	CVE-2023-46850	9.8	A vulnerability in the OpenVPN version used by this product	Update to V3.2 SP2
User Management Component (UMC)	CVE-2024-33698	9.8	A buffer overflow vulnerability leading to code execution	Siemens provided Updates and advised filtering ports 4002, 4004 for UMC.
SINEC NMS	CVE-2024-41940	9.1	Improper input validation leads to OS command execution with elevated privileges	Update to V3.0
SCALANCE, RUGGEDCOM, SIPLUS, and SINEC	CVE-2024-3596	9.0	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks	Restrict access to the network Configure theRADIUS server to require amessage authenticator For SCALANCE Update to V4.1.8
SINEMA Remote Connect Server	CVE-2024-39872	9.6	Privilege escalation Vulnerability in temporary files created by product	Update to V3.2 SP1
SICAM CPCI85	CVE-2024-37998	9.8	Administrative password resets without the current password	Update to V5.40
SIMATIC SCADA and PCS 7	CVE-2024-35783	9.1	The product DB Runs with elevated privileges	Update to V7.5 SP2 Update 18 or V8.0 Update 5
SCALANCE W700	CVE-2023-44373	9.1	The product DB Runs with elevated privileges	Update to V2.4.0

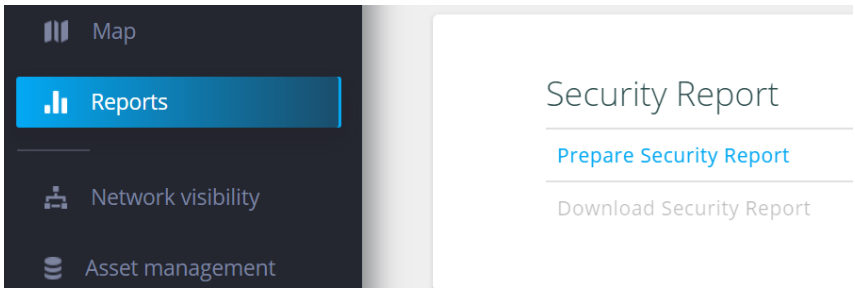
VIESMANN

Product	CVE	CVSS	details	Mitigation
Vitogate 300	CVE-2023-5222	9.8	Hard-coded password in versions 2.1.3.0 and prior	Update to version 3.0.0.0
Vitogate 300	CVE-2023-45852	9.8	Authentication bypass vulnerability in versions 2.1.3.0 and prior	Update to version 3.0.0.0

Product	CVE	CVSS	details	Mitigation
Cisco Smart Licensing Utility	CVE-2024-20439	9.8	When the product is actively running an unauthenticated attacker can collect data or administer services	Update to a fixed release 2.3.0
	CVE-2024-20440	9.8		
Smart Software Manager On-Prem	CVE-2024-20419	10.0	Due to improper implementation of the password-change process, an attacker can change the password of any user, including the admin.	Update to a fixed release 8-202212 or version 9

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 ensure 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.

CIARA Threat Intelligence Updates

We enhanced our Threat Intelligence capabilities by adding **5** new cyber threat groups to CIARA and updating information on **11** existing groups.

Threat groups added

Velvet Ant

We added Velvet Ant to our threat intelligence following an incident response research released by Sygnia, revealing their zero-day vulnerability exploitation. This China-nexus threat group is known for targeting critical infrastructure using advanced malware and espionage tactics, posing a high-risk threat.

RansomHub

Following a recent cyber-attack on oil and gas services giant Halliburton by RansomHub, and in light of an advisory released by CISA and other agencies, we added RansomHub to our threat intelligence. This ransomware-as-a-service group uses a double-extortion model, encrypting data while exfiltrating it, and threatening to publish stolen information if the ransom is not paid.

ColdRiver

This group was added as part of Radiflow's efforts to track cyber-attack groups active in the Russia-Ukraine war, enhancing our threat intelligence on key actors involved.

GhostWriter

This group was added as part of Radiflow's efforts to track cyber-attack groups active in the Russia-Ukraine war, enhancing our threat intelligence on key actors involved.

FrostyGoop

FrostyGoop is an ICS-specific malware, notable for using the Modbus TCP protocol to communicate with industrial control devices. FrostyGoop can read and write to device registers and was used in a cyberattack in Ukraine, which disrupted heating services to over 600 buildings for two days.

Threat groups updated

APT28, Sandworm, TEMP.Veles, Turla, APT29

These groups were updated as part of Radiflow's efforts to track cyber-attack groups involved in the Russia-Ukraine war and their recent activities. These updates further enhance our threat intelligence on key actors within the conflict.

SideWinder

This group was updated following the discovery of a new campaign targeting ports and maritime facilities. The goal of this campaign is espionage and intelligence gathering.

APT41

This group was updated following Google's Threat Analysis Group (TAG) and Mandiant's discovery of a new campaign targeting global shipping and logistics, technology, and automotive sectors. APT41 has infiltrated and maintained persistent access to victim

networks, enabling extensive espionage activities and the extraction of sensitive data over an extended period.

Ember Bear

This group was updated following the CISA advisory, which highlighted new activities by Ember Bear. Ember Bear is a suspected Russian state-sponsored cyber espionage group, actively targeting critical infrastructure sectors, particularly focusing on government services, transportation, and energy in NATO and EU countries.

APT33

The threat group profiles and techniques were updated following Microsoft's discovery of APT33's use of a new backdoor called Tickler. APT33 is an Iranian state-sponsored cyber group known for intelligence-gathering and destructive operations. They are particularly active in sectors such as satellite communications, oil and gas, and government organizations.

Volt Typhoon

The threat group profiles and techniques were updated following the recent exploitation of a zero-day vulnerability in Versa Director, which targeted U.S. ISPs. Volt Typhoon, a China-backed APT group, is known for targeting critical infrastructure sectors, including communications, manufacturing, and government organizations.

Fox Kitten

The threat group profiles and techniques were updated following the recent advisory from CISA, which details Fox Kitten an Iranian state-sponsored cyber actor collaborating with ransomware affiliates targeting U.S. organizations across sectors. Their tactics involve exploiting vulnerabilities in public-facing networking devices to gain initial access, after which they enable ransomware operations.

Threat Group	Techniques	Industry	Country	Region	Aliases
APT28	V	V	V	V	X
Sandworm Team	V	V	X	X	X
Side Winder	V	X	V	X	X
APT41	V	V	V	V	X
TEMP.Veles	V	X	X	X	X
Turla	V	V	X	X	X
Ember Bear	V	V	V	V	V
APT33	V	V	V	V	V
Volt Typhoon	V	X	X	X	X
Fox Kitten	V	V	V	V	V
APT29	V	V	V	V	X

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 to obtain the CIARA update files, please contact our team at support@radiflow.com or visit our official website at Radiflow.com.

Additional Info

https://www.cisa.gov/news-events/ics-advisories/icsa-24-184-02
https://www.cisa.gov/news-events/ics-advisories/icsa-24-193-18
https://www.cisa.gov/news-events/ics-advisories/icsa-24-226-02
https://www.cisa.gov/news-events/ics-advisories/icsa-24-226-05
https://www.cisa.gov/news-events/ics-advisories/icsa-24-242-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-22
https://www.cisa.gov/news-events/ics-advisories/icsa-24-193-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-193-05
https://www.cisa.gov/news-events/ics-advisories/icsa-24-228-06
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-10
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-11
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-13
https://www.cisa.gov/news-events/ics-advisories/icsa-24-256-14
https://www.cisa.gov/news-events/ics-advisories/icsa-24-207-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-254-01
https://www.sygnia.co/blog/china-nexus-threat-group-velvet-ant/
https://www.bleepingcomputer.com/news/security/halliburton-cyberattack-linked-to-ransomhub-ransomware-gang/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a
https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf
https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology
https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a
https://www.microsoft.com/en-us/security/blog/2024/08/28/peach-sandstorm-deploys-new-custom-tickler-malware-in-long-running-intelligence-gathering-operations/
https://therecord.media/versa-zero-day-volt-typhoon-china
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-auth-sLw3uhUy