Radiflow

Quarterly ICS Security Report
2024 Q1

Radiflow

Contents

Executive Summary 3
ICS Cybersecurity Incidents 4
ICS Vulnerabilities 5
CISA ICS Advisories 6
Visibility 8
Radiflow's additional best practice recommendations 8
CIARA Threat Intelligence Updates 9
Ongoing Support 9
Additional Info 10

Radiflow

Executive Summary

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

Radiflow

ICS Cybersecurity Incidents

Manufacturing 

VARTA

In February, VARTA AG, a prominent German battery manufacturer, was targeted by a sophisticated and organized group of unknown hackers, resulting in a significant cyberattack. This attack led to the shutdown of IT systems and the suspension of production at the company's global facilities located in Germany, Romania, and Indonesia, broadly affecting VARTA AG's operations and severely impacting the company's finances

Schneider Electric

In mid-January, Schneider Electric was hit by a ransomware attack from the Cactus cybercrime group, targeting its sustainability business division. The breach, which compromised the EcoStruxure Resource Advisor platform, did not affect safety-critical systems but posed risks of client business data leaks.

thyssenkrupp

In February, Thyssenkrupp, a German steelmaking conglomerate, experienced a ransomware attack. Attackers exploited vulnerabilities, gaining unauthorized access to the company's data and systems. This led to a temporary halt in production across various operational sites, causing significant disruptions in the company's supply chain.

Water and Wastewater 

water for people
EVERYONE • FOREVER

In March, the Medusa ransomware gang targeted the nonprofit Water for People, dedicated to providing clean water in the world's poorest regions. Although the attack occurred, Water for People assured that the compromised data was outdated (pre-2021), their financial systems were unaffected, and their operations continued without interruption. This incident highlights the broader trend of Medusa ransomware operations targeting the water company sector.

VEOLIA

In mid-January, Veolia North America's Municipal Water division encountered a ransomware attack, affecting specific software applications and systems. The company quickly implemented countermeasures, preventing any disruption to its water or wastewater treatment operations. The breach was limited to internal back-end systems, with a possibility of affecting a small group of individuals' personal information.

Radiflow

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 Q1 of 2024.

Total new vulnerabilities in Q1: **8,637**

ICS vulnerabilities among these: **94**

Older vulnerabilities discovered in ICS devices: **538**

severity	CVEs
Critical	75
High	332
Medium	209
Low	16

Total new CISA KEVs (Known Exploited Vulnerabilities) in Q1 of 2024: **40**

ICS Vulnerabilities Within CISA KEV: **6**

CVE	CVSS	Vendor	Product
CVE-2019-7256	10	Nice	Linear eMerge E3-Series
CVE-2023-27997	9.8	Siemens	RUGGEDCOM APE1808
CVE-2024-21762	9.8	Siemens	RUGGEDCOM APE1808
CVE-2023-44487	7.5	Siemens	RUGGEDCOM APE1808
CVE-2022-41328	6.7	Siemens	RUGGEDCOM APE1808
CVE-2021-0920	6.4	Siemens	SIMATIC

Radiflow

CISA ICS Advisories

Total new CISA ICS advisories in Q1 of 2024: **83**.

Notable ICS Vulnerabilities:

UNITRONICS®

Affected Product	CVE	CVSS	Mitigation
Unistream Unilogic – Versions prior to 1.35.227	CVE-2024-27767	10	1. Monitor communication on TCP port 20256 from external IP 2. Update Unilogic software to version 1.35.227.
	CVE-2024-27768	9.8	
	CVE-2024-27769	8.8	
	CVE-2024-27770	8.8	
	CVE-2024-27771	8.8	
	CVE-2024-27772	8.8	
	CVE-2024-27773	8.8	
	CVE-2024-27774	7.5	

SIEMENS

Affected Product	CVE	CVSS	Mitigation
SIMATIC CN 4100	CVE-2023-49621	9.8	Update to V2.7 or a later version.
SIMATIC, with maxView	CVE-2023-51438	10	Update maxView to V4.14.00.26068 or a later version.
SCALANCE W1750D	CVE-2023-45614	9.8	1. Monitor communication on UDP port 8211 from external IP 2. Enable cluster security via the cluster-security command
	CVE-2023-45615	9.8	
	CVE-2023-45616	9.8	
RUGGEDCOM APE1808, with Fortinet's NGFW	CVE-2024-21762	9.8	Update Fortigate NGFW to V7.4.1.
	CVE-2024-23113	9.8	
	CVE-2023-25610	9.8	Disable HTTP/HTTPS administrative interface OR Limit access
	CVE-2023-27997	9.8	Disable SSL-VPN
	CVE-2023-33308	9.8	Disable HTTP/2 support on SSL inspection profiles

Affected Product	CVE	CVSS	Mitigation
Wire-cut EDM and Sinker EDM	CVE-2023-21554	9.8	For information about an update, please contact your local Mitsubishi Electric service center
MELSEC-Q/L Series controllers	CVE-2024-0802	9.8	Mitsubishi Electric is working on an update for this issue and recommends the following: • Use a firewall or VPN • Restrict access to the affected product • Install antivirus software
	CVE-2024-0803	9.8	
	CVE-2024-1915	9.8	
	CVE-2024-1916	9.8	
	CVE-2024-1917	9.8	

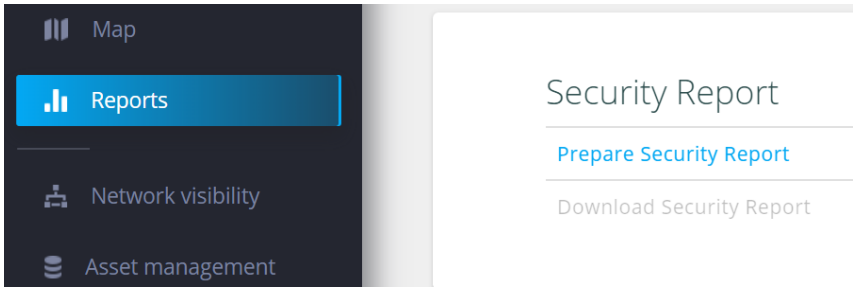
Affected Product	CVE	CVSS	Mitigation
FactoryTalk Service Platform: Versions prior to v6.4	CVE-2024-21917	9.8	• Update to FTSP v6.40 or later • Set DCOM authentication level to 6 • Enable verification of the publisher information (digital signature) of any executable attempting to use the FactoryTalk Services APIs

Affected Product	CVE	CVSS	Mitigation
Rosemount gas chromatograph models GC370XA, GC700XA, and GC1500XA, running software version 4.1.5 or earlier,	CVE-2023-46687	9.8	Emerson released a firmware update, For update information, contact Emerson Tech Support

Radiflow

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.

Radiflow

CIARA Threat Intelligence Updates

We added 5 new threat groups to CIARA and updated 7 existing groups.

Threat groups added

AlphV

CISA has released an advisory as part of an ongoing operation to #StopRansomware. The AlphV ransomware group is known for targeting critical infrastructure using advanced social engineering and employing tactics like data exfiltration and double extortion threats.

Play

CISA has released an advisory as part of an ongoing operation to #StopRansomware. The Play ransomware group is known for targeting critical infrastructure, employing a double-extortion model, and encrypting systems after exfiltrating data.

Rhysida

CISA has released an advisory as part of an ongoing operation to #StopRansomware. The Rhysida ransomware group is known for targeting manufacturing, government, and healthcare industries.

Medusa

Medusa Ransomware is an active cyber threat group, targeting corporate victims, employing a double-extortion tactic.

Desorden

Desorden is an active cyber threat group targeting the APAC region. They exfiltrate data and threaten to publicize it unless a ransom is paid.

Threat groups updated

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

Threat Group	Techniques	Industry	Country	Region	Aliases
Dragonfly	V	V	V	V	V
APT17	V	V	V	V	V
LockBit	V	X	X	X	X
APT29	V	V	V	V	V
Mustang Panda	V	V	V	V	V
Lotus Blossom	V	V	V	V	V
Magic Hound	V	V	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.

Radiflow

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://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a
https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/#post-131837-_7datli60tj7t
https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Desorden&n=1
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a
https://andreacristaldi.github.io/APTmap/#name=APT29&
https://andreacristaldi.github.io/APTmap/#name=Dragonfly&
https://andreacristaldi.github.io/APTmap/#name=APT%2017&
https://andreacristaldi.github.io/APTmap/#name=Mustang%20Panda&
https://andreacristaldi.github.io/APTmap/#name=Lotus%20Panda&
https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1134040
https://www.cisa.gov/news-events/ics-advisories/icsa-24-030-06
https://www.cisa.gov/news-events/ics-advisories/icsa-24-011-09
https://www.cisa.gov/news-events/ics-advisories/icsa-24-011-10
https://www.cisa.gov/news-events/ics-advisories/icsa-24-030-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-046-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-051-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-074-05
https://www.cisa.gov/news-events/ics-advisories/icsa-24-074-11
https://www.cisa.gov/news-events/ics-advisories/icsa-24-074-14