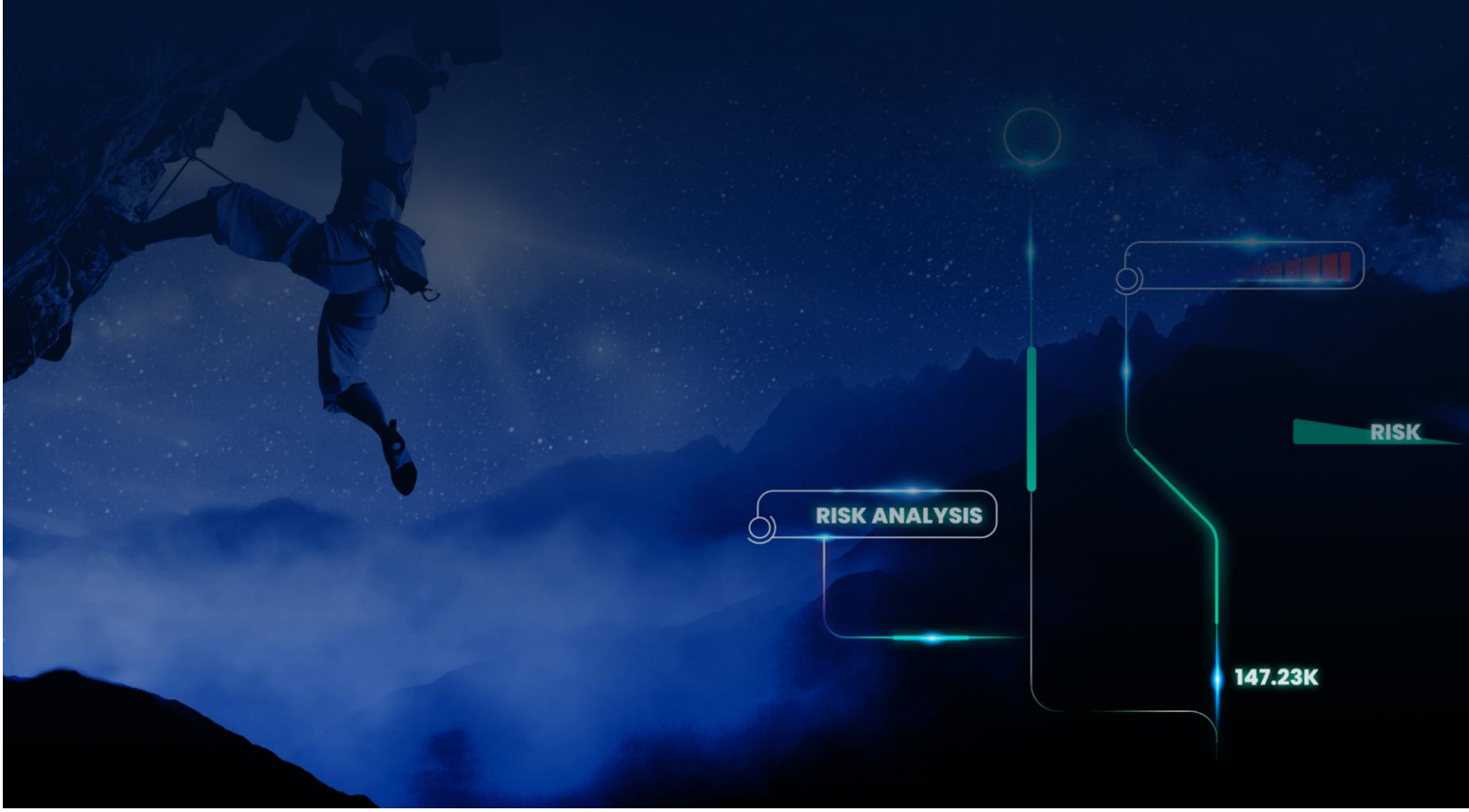
Radiflow

Quarterly ICS Security Report
2024 Q2



Radiflow

Contents

Radiflow

Executive Summary

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

nexperia

In April 2024, the Dark Angels (Dunghill) ransomware group claimed to have stolen 1 Tb of data from Nexperia, a Netherlands-based semiconductor company owned by China's Wingtech Technology. The stolen data reportedly includes quality control information, client folders, and confidential project data. The ransomware group announced the theft on its Tor-based site, releasing some files as proof and threatening to leak all the data unless a ransom is paid.

МОСКОЛЛЕКТОР

The BlackJack hacker group, possibly linked to Ukrainian intelligence, launched a cyberattack on April 9th against Moscow's "Moscollector" industrial sensor and monitoring infrastructure. This system manages the safety of municipal services like gas, water, and fire alarms. The attackers deployed the Fuxnet malware, disrupting around 87,000 sensors and control systems, and destroying about 1,700 sensors and routers. They wiped 30TB of critical data from servers and workstations, leaked sensitive data from the Network Operation Center (NOC), and defaced Moscollector's website and Facebook account. The Radiflow research team analyzed the attack; the detailed report can be viewed here.

SolidCAM

In June 2024, the Handala ransomware group announced it had successfully hacked SolidCAM, a prominent provider of integrated CAD/CAM solutions, claiming to have accessed over 800GB of data. SolidCAM, known for its computer-aided manufacturing software used in sensitive industries like aerospace and drone production, was allegedly infiltrated for months. Handala stated that they used SolidCAM's network to spread their backdoor tool and threatened to publish the stolen data if the company did not respond honestly. The group hinted at broader implications, linking their activities to recent accidents and explosions.

In May 2024, the German and Czech governments disclosed a sophisticated cyber espionage campaign by Russian military intelligence, targeting political parties and critical infrastructure. The GRU hackers, known as APT28 or Fancy Bear, exploited a zero-day vulnerability in Microsoft Outlook to infiltrate networks. The campaign, which began in 2023, focused on sectors such as energy, logistics, aerospace, and IT services.

keytronic

On June 18, 2024, Key Tronic, a contract manufacturer and printed circuit board assembly (PCBA) giant, confirmed a ransomware attack by the Black Basta group, which leaked 530GB of stolen data. The incident, which occurred on May 6, 2024, caused widespread operational disruptions, leading the company to suspend operations in the US and Mexico for two weeks.

Russia-linked hackers, identified as the Sandworm group, have claimed responsibility for cyberattacks on water utilities in the United States, France, and Poland. The attacks included manipulating systems causing a water tower overflow in Muleshoe, Texas, and targeting a wastewater utility in Poland. In March, the group also claimed to have compromised a French hydroelectric power station

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 Q2 of 2024.

Total new vulnerabilities in Q2: **11,714**

ICS vulnerabilities among these: **189**

Older vulnerabilities discovered in ICS devices: **174**

severity	CVEs
Critical	42
High	202
Medium	111
Low	8

Total new CISA KEVs (Known Exploited Vulnerabilities) in Q2 of 2024: **33**

ICS Vulnerabilities Within CISA KEV: **5**

CVE	CVSS	Vendor	Product
CVE-2024-3400	10	Apache	ActiveMQ
CVE-2023-46604	9.8	Palo Alto Networks	PAN-OS
CVE-2022-0028	8.6	Palo Alto Networks	PAN-OS
CVE-2023-38180	7.5	IETF	HTTP/2
CVE-2023-44487	7.5	Microsoft	.NET Core and Visual Studio

Radiflow

CISA ICS Advisories

Total new CISA ICS advisories in Q2 of 2024: **94**.
Notable ICS Vulnerabilities:

SIEMENS

Product	CVE	CVSS	details	Mitigation
RUGGEDCOM APE1808	CVE-2022-0028	8.6	A CISA-KEV in PAN-OS used in RUGGEDCOM	Upgrade Palo Alto Networks Virtual NGFW to V11.0.1
RUGGEDCOM APE1808	CVE-2023-51438	10	A CISA-KEV in the GlobalProtect feature of Palo Alto Networks PAN-OS software	Contact customer support to receive patch and update information. Disable GlobalProtect gateway and GlobalProtect portal
ST7 ScadaConnect	CVE-2023-38180	7.5	A CISA-KEV Denial-of-Service Vulnerability in .NET and Visual Studio	Update ST7 ScadaConnect to V1.1 or later version
ST7 ScadaConnect	CVE-2023-44487	7.5	A CISA-KEV Denial-of-Service Vulnerability in the HTTP/2 protocol	Update ST7 ScadaConnect to V1.1 or later version
SIMATIC CN 4100	CVE-2024-32740	9.8	Use of hard-coded credentials and password	Update to V3.0 or later version
	CVE-2024-32741	10.0		
SIMATIC RTLS Locating Manager	CVE-2024-30207	10.0	Use of symmetric cryptography with a hard-coded key	update to V3.0.1.1 or later version
	CVE-2024-30209	9.6	The systems transmit client-side resources without proper cryptographic protection	
	CVE-2024-33499	9.1	The application assigns incorrect permissions to a user management component	
RUGGEDCOM CROSSBOW	CVE-2024-27939	9.8	The affected systems allow the upload of arbitrary files by any unauthenticated user	update to v5.5 or later version
Desigo and Cerberus	CVE-2024-22039	10.0	An RCE vulnerability caused by The network communication library, not validating the size of the input	Update to the latest version MP4 or V4.3.0001
Scalance W1750D	CVE-2023-35980	9.8	An RCE vulnerability caused by buffer overflow in multiple services	Update to V8.10.0.9 or later version
	CVE-2023-35981	9.8		
	CVE-2023-35982	9.8		

Radiflow

EMERSON

Product	CVE	CVSS	details	Mitigation
Ovation	CVE-2022-29966	9.8	An RCE and denial-of-service vulnerability caused by lack of authentication and data verification	Upgrade to the currently available release of Ovation 3.8.0 Feature Pack 3
	CVE-2022-30267	9.1		

DELTA

Product	CVE	CVSS	details	Mitigation
InfraSuite Device Master	CVE-2023-46604	9.8	A CISA-KEV in Apache ActiveMQ (5.15.2) which is used by InfraSuite Device Master	update to version 1.0.11 or later

AUTOMATIONDIRECT.com

Product	CVE	CVSS	details	Mitigation
Productivity PLCs	CVE-2024-23601	9.8	These vulnerabilities can allow a malicious actor to execute code remotely and create a denial-of-service attack	Update the Productivity Suite programming software to version 4.2.0.x or higher. Update Productivity PLC's firmware to the latest version.
	CVE-2024-21785	9.8		
	CVE-2024-22187	9.1		
	CVE-2024-24963	9.8		
	CVE-2024-24962	9.8		

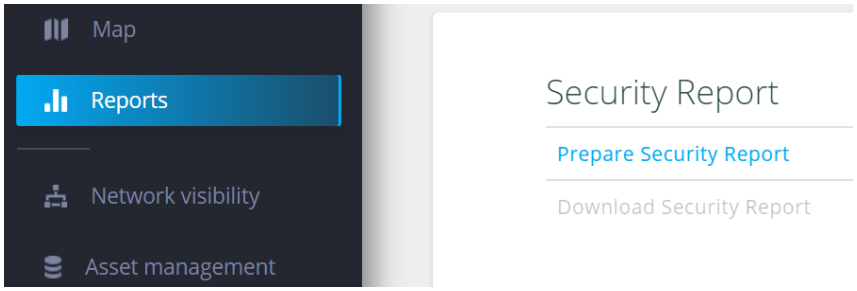
westermo

Product	CVE	CVSS	details	Mitigation
Westermo EDW-100	CVE-2024-36080	9.8	Hidden administrator account with a hardcoded password	EDW-100 functions as an industrial serial to ethernet converter, so there are no built-in protective measures. Westermo recommends the use of network segregation and perimeter protection or replacing EDW-100 with Lynx DSS L105-S1
	CVE-2024-36081	9.8	An unauthenticated GET request can download the configuration file containing the configuration, username, and passwords in clear text.	

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

MITRE has released an update to ATT&CK v15, introducing new techniques and groups, and updating techniques for existing groups. This update includes 12 new groups and updated techniques for 65 existing groups. The update was added to the CIARA signatures file, along with three new threat groups and updates for three existing groups from Radiflow's research team.

Threat groups added

BlackJack

The hacker group BlackJack, possibly linked to Ukrainian intelligence, launched a coordinated cyberattack against Moscow's "Moscollector" infrastructure, deploying Fuxnet malware. For more information see Radiflow Analysis.

ArcaneDoor

ArcaneDoor is a state-sponsored campaign targeting perimeter network devices from multiple vendors. The attackers use these devices as intrusion points for espionage, exploiting vulnerabilities to modify traffic and monitor communications.

FlightNight

FlightNight is a new cyber espionage group targeting the government and energy sectors. They launched a phishing attack on Indian entities, exfiltrating 881 GB of data.

Threat groups updated

Common Hacktivists

The US Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the FBI and NSA, issued a warning about pro-Russia hacktivists targeting OT systems and critical infrastructure. For more information see Radiflow Blog.

Kimsuky

The threat group profiles and techniques were updated Following recent activities.

Sandworm

The threat group profiles and techniques were updated Following recent activities.

Threat Group	Techniques	Industry	Country	Region	Aliases
BlackJack	V	V	V	V	X
ArcaneDoor	V	V	V	V	V
FlightNight	V	V	V	V	X
Kimsuky	V	V	V	V	V
Sandworm	V	V	V	V	V
Common Hacktivists	V	X	X	X	X

Radiflow

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 reach out to our team at support@radiflow.com or visit our official website at Radiflow.com.

Additional Info

https://www.radiflow.com/radiflow-labs/cisa-warns-about-threat-actors-targeting-critical-national-infrastructure/

https://www.radiflow.com/radiflow-labs/ukrainian-blackjack-apt-attack-on-moscow-ot-infrastructure-fuxnet/

https://attack.mitre.org/resources/updates/

https://www.cisa.gov/news-events/ics-advisories/icsa-24-144-01
https://www.cisa.gov/news-events/ics-advisories/icsa-24-130-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-158-02
https://www.cisa.gov/news-events/ics-advisories/icsa-24-102-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-116-03
https://www.cisa.gov/news-events/ics-advisories/icsa-24-137-06
https://www.cisa.gov/news-events/ics-advisories/icsa-24-137-07
https://www.cisa.gov/news-events/ics-advisories/icsa-24-137-10
https://www.cisa.gov/news-events/ics-advisories/icsa-24-137-12
https://www.cisa.gov/news-events/ics-advisories/icsa-24-102-05
https://www.cisa.gov/news-events/ics-advisories/icsa-24-165-04
https://www.cisa.gov/news-events/ics-advisories/icsa-24-151-04