2025 May, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, podcasts, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents

ICS good practices, recommendations

Improve Password Hygiene: Strategic Authentication Management for Industrial Systems

May 1st is World Password Day in 2025. A recent entry on the TeamPassword Blog addresses the security of passwords in Industrial Control Systems (ICS), which remains a complex and challenging topic. We recommend reviewing this section of the blog and evaluating which aspects may be applicable and implementable within our organization.

Password management in industrial control systems involves unique challenges stemming from legacy systems, shared workstations, and operational requirements that don't align well with traditional IT password policies. An effective ICS password strategy must balance security requirements with operational realities.

Industrial-Specific Password Challenges and Solutions:

Legacy Systems with Limited Authentication Options: Many older control systems have significant password limitations - some accept only numeric passwords, have maximum length restrictions, or don't support special characters. Others store passwords in plaintext or use weak hashing algorithms.

For these systems:

- Implement compensating controls like network isolation and strict access control
- When possible, place authentication proxies in front of systems with weak password mechanisms
- For devices that cannot support strong passwords, implement physical security controls to prevent direct access

Default and Hardcoded Credentials: Industrial devices often ship with default credentials documented in publicly available manuals. Worse, some have hardcoded passwords that cannot be changed.

Address this by:

- Creating a comprehensive default credential inventory during commissioning
- Changing all changeable default passwords immediately upon installation
- Isolating devices with unchangeable credentials into strictly controlled network segments
- Using network-based controls to restrict authentication attempts to these devices

Shared Workstation and Credential Management: Control rooms and operator stations are typically shared among multiple personnel across shifts, complicating individual accountability.

Effective approaches include:

- Implementing time-synchronized shift-change password procedures
- Using role-based rather than individual accounts for operator functions, with enhanced logging
- Deploying industrial-focused privileged access management (PAM) solutions that vault credentials for shared systems
- Creating audit mechanisms that associate specific actions with individuals through secondary authentication for critical operations

Emergency Access Procedures: Industrial environments require rapid response during emergencies, when normal authentication processes might impede necessary actions.

Design emergency authentication with:

- Physical break-glass procedures that provide emergency credentials
- Automated notifications when emergency credentials are used
- Post-incident auditing and credential rotation
- Regular drills to ensure emergency authentication processes function correctly

Password Rotation Strategies: Traditional 90-day password rotation isn't always practical in industrial environments where system access is infrequent but critical.

Consider alternatives like:

- Event-based rotation (after vendor maintenance or personnel changes) rather than time-based rotation
- Using longer, more complex passwords with less frequent rotation for rarely accessed systems
- Implementing one-time passwords for vendor and contractor access
- Separating standard operational passwords from administrative credentials, with stricter policies for the latter

By developing password policies specifically designed for industrial operational realities, you create security that enhances rather than hinders essential functions while still providing effective protection against unauthorized access.

Source (the TeamPassword solution recommendation) and more detailed information available on the following link:

https://www.enisa.europa.eu/publications/enisa-nis360-2024

ICS conferences

In June 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

ICS Security Summit & Training 2025

The 20th Annual SANS ICS Security Summit will be an event to remember! Held at Disney World, this milestone gathering offers something for everyone - from introductory learning for those new to ICS/OT security to advanced insights and techniques for seasoned practitioners. Experience in-depth talks, immersive hands-on workshops, and practical takeaways led by the industry's top experts.

Create core memories with your peers in the ICS/OT community and your family during a magical getaway. Extend the experience with world-class training courses immediately after the Summit to further build your expertise.

Lake Buena Vista, FL, US and Virtual - ET; 3-Day Summit: 15th -17th June | Courses: 18th -23rd June 2025

More details can be found on the following website:

https://www.sans.org/cyber-security-training-events/ics-security-summit-2025/

OT Cybersecurity Summit

Threat Intelligence plays a crucial role in the ongoing advancement of automation by enabling the development of more sophisticated, adaptive, and efficient systems. As automation technologies continue to evolve, integrating advanced intelligence capabilities, such as machine learning, artificial intelligence and predictive analytics, is becoming increasingly important. As the industrial landscape rapidly evolves, ensuring the security of operational technology (OT) systems is paramount. A critical component of this is safeguarding the supply chain, which has become a prime target for cybercriminals seeking to exploit vulnerabilities.

Focus on enhancing the security of your network and information systems and build confidence in your OT cybersecurity plan and learn to anticipate new challenges.

Brussels, Belgium; 18th – 21st June 2025

More details can be found on the following website:

https://otcs.isa.org/

23rd Global Edition OTSEC MENA

With the steady adoption of IoT and personal connected devices, it's reported an increase of over 4-fold in IoT malware attacks year-over-year in the Middle East region. The growth in cyber threats demonstrates cyber criminals' persistence and ability to adapt to evolving conditions in launching IoT malware attacks.

Cybercriminals are targeting legacy vulnerabilities, with 34 of the 39 most popular IoT exploits specifically directed at vulnerabilities that have existed for over three years. The biggest receiver of these attacks has been manufacturing, followed by oil & gas, Power grids and maritime.

Secured Managed Services and Ai will play a key role in the future of cyber security; however, it remains that it's not the task of the security team alone. It's an effort by everyone working within those organisations.

Join CISOs, Heads of OT and ICS Security from MENA region on 24th-25th June 2025, Saudi Arabia, to discuss key challenges and opportunities in OT, IOT, IIOT & IOMT Cyber Security for Critical Infrastructure and key sectors at OTSEC MENA SUMMIT & AWARDS 2025.

Al Khobar, Saudi Arabia; 24th – 25th June 2025

More details can be found on the following website:

https://otsecsummit.com/#

ICS incidents

Ransomware Attack Hits Sensata Technologies, Disrupting Global Operations

Massachusetts-based industrial technology manufacturer Sensata Technologies experienced a significant ransomware attack over the weekend, resulting in widespread disruption to its operations, including production outages.

In a disclosure to the U.S. Securities and Exchange Commission (SEC), Sensata confirmed that the attack began on another day and led company officials to take entire network systems offline to contain the damage. The incident has impacted several critical business areas, such as manufacturing production, shipping, receiving, and various support functions. While interim measures have been put in place to restore limited functionality, a timeline for full recovery remains uncertain.

The company's preliminary internal investigation revealed that attackers were able to exfiltrate files from the corporate network. Cybersecurity experts have been engaged to assist in containment, recovery, and the identification of stolen data. Notifications will be issued should any personal or sensitive data be confirmed as compromised.

Sensata, which operates in a dozen countries and employs over 19,000 people, produces sensors, electrical protection devices, and control systems across the automotive, aerospace, heavy equipment, and industrial sectors. With annual revenues nearing $4 billion, the company ships roughly 1 billion products annually.

While Sensata currently does not anticipate a material financial impact from the attack this quarter, it acknowledged that this assessment may change depending on the extent of the disruption and ongoing recovery efforts. Importantly, the production halt - along with other operational delays - could have cascading effects across its global supply chains.

As of the latest update, no ransomware group has claimed responsibility for the attack.

The source is available on the following link:

https://therecord.media/sensata-technologies-ransomware-attack

Cyber attack disrupts operational systems at South African Airways

On May 3rd, 2025, South African Airways (SAA) experienced a major cyber incident that temporarily disrupted access to its website, mobile app, and several internal systems. The airline swiftly activated its disaster recovery and business continuity plans, which effectively contained the incident and minimized disruption to flight operations. Essential customer services, including contact centers and sales offices, remained functional, and normal system operations were restored the same day.

SAA launched a thorough investigation with independent digital forensic experts to determine the root cause and assess the extent of the breach. The possibility of external cybercriminal activity is being explored. While it remains unclear whether personal data was accessed or exfiltrated, SAA has committed to notifying affected parties in accordance with regulatory requirements if a data breach is confirmed.

John Lamola, Group CEO of SAA, reassured stakeholders of the airline's commitment to cybersecurity and operational resilience. He emphasized that SAA is taking all necessary steps to strengthen its security framework and mitigate future risks.

As a National Key Point, SAA reported the incident to the State Security Agency (SSA), South African Police Service (SAPS), and the Information Regulator, in compliance with the Protection of Personal Information Act (POPIA).

The SAA incident follows a growing trend of cyberattacks in South Africa in early 2025. MTN Group recently disclosed a data breach affecting customer information, though core systems remained secure. Other victims of cyberattacks this year include the national weather service, the country's largest poultry producer, and major tech firm Masimo Corporation, which reported unauthorized access affecting its manufacturing systems in late April.

These incidents highlight the growing cybersecurity challenges faced by key industries in South Africa.

The source is available on the following link:

Cyber attack disrupts operational systems at South African Airways - Industrial Cyber

Book recommendation

Cybersecurity in the Electricity Sector: Managing Critical Infrastructure

This book offers a systematic explanation of cybersecurity protection of electricity supply facilities, including discussion of related costs, relevant standards, and recent solutions. The author explains the current state of cybersecurity in the electricity market, and cybersecurity standards that apply in that sector. He then offers a systematic approach to cybersecurity management, including new methods of cybersecurity assessment, cost evaluation and comprehensive defence.

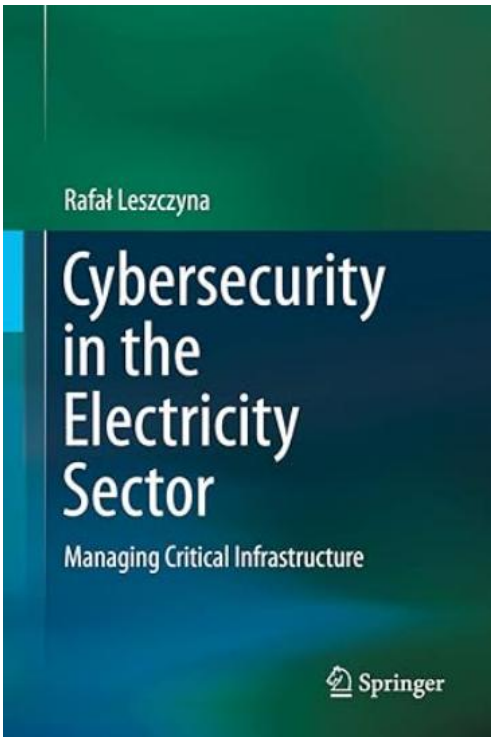
This monograph is suitable for practitioners, professionals, and researchers engaged in critical infrastructure protection.

Author/Editor: Rafał Leszczyna (Author)

Year of issue: 2019

The book is available at the following link:

https://www.amazon.com/Cybersecurity-Electricity-Sector-Managing-Infrastructure/dp/3030195376



ICS security news selection

Many Fuel Tank Monitoring Systems Vulnerable to Disruption

RSAC CONFERENCE 2025 – San Francisco – Internet-connected automatic tank gauges (ATGs) pose a serious but often overlooked cyber-risk to the thousands of gas stations, fuel depots, and facilities that rely on these devices to monitor tank levels, temperatures, leaks, and other critical operational parameters.

Pedro Umbelino, principal research scientist at Bitsight, is sounding the alarm on the issue at the 2025 RSAC Conference this week, warning that hackers could cause considerable chaos by tampering with ATGs. …

Source and more information:

https://www.darkreading.com/ics-ot-security/fuel-tank-monitoring-systems-vulnerable-disruption

Build More Robust OT Security With the NIST Framework

To combat escalating risks, numerous organizations look to the US National Institute of Standards and Technology (NIST) Cybersecurity Framework to protect their operational technology (OT) environments. It rests on six interrelated functions: Identify, Protect, Detect, Respond, Recover, and Govern.

The NIST Cybersecurity Framework: A Strategic Approach

To apply the NIST Cybersecurity Framework successfully, you need to understand its six functions. …

Source and more information:

https://www.darkreading.com/ics-ot-security/build-more-robust-ot-security-nist-framework

ISA-95 standard updated to integrate enterprise and manufacturing control systems

The International Society of Automation published Apr. 10 its ANSI/ISA-95.00.01-2025 (IEC 62264-1 Mod), "Enterprise-control system integration—part 1: models and terminology." This is the latest update of the ISA-95 series, which are widely used,

international standards that describe how to integrate logistics systems with manufacturing control systems.

ANSI/ISA-95.00.01-2025, also known as ISA-95 Part 1, summarizes the scope of the manufacturing operations and control domain, discusses how physical assets of a manufacturing enterprise are organized, lists the functions associated with the interface between control functions and enterprise functions, and describes the information shared among these functions. …

Source and more information:

https://www.controlglobal.com/industry-news/news/55287684/isa-95-standard-updated-to-integrate-enterprise-and-manufacturing-control-systems

ICS/OTUS Warns of Hackers Targeting ICS/SCADA at Oil and Gas Organizations

Agencies say the attacks leverage basic intrusion techniques, but poor cyber hygiene within critical infrastructure organizations could lead to disruptions and damage.

The US cybersecurity agency CISA, the FBI, EPA, and the DoE on Tuesday issued an alert to warn organizations of cyberattacks targeting the country's oil and natural gas sector.

The observed attacks, the government agencies say, leverage basic intrusion techniques, but poor cyber hygiene within critical infrastructure organizations could lead to disruptions and even physical damage.

"CISA is increasingly aware of unsophisticated cyber actor(s) targeting ICS/SCADA systems within U.S. critical Infrastructure sectors (Oil and Natural Gas), specifically in Energy and Transportation Systems," the cybersecurity agency notes. …

Source and more information:

https://www.securityweek.com/us-warns-of-hackers-targeting-ics-scada-at-oil-and-gas-organizations/

Unimicron, Presto Attacks Mark Industrial Ransomware Surge

A number of major industrial organizations suffered ransomware attacks last quarter, such as PCB manufacturer Unimicron, appliance maker Presto, and more — a harbinger of a rapidly developing and diversifying threat landscape.

Attacks on major organizations such as Unimicron, the South African Weather Service (SAWS), National Presto Industries, and Lee Enterprises signaled a surge in ransomware across critical infrastructure sectors in the first quarter of 2025 — a trend that was exacerbated by a growth in the variety and sophistication of the tactics used.

That's according to security vendor Dragos, which noted in a report, released today, on attacks on critical infrastructure that ransomware is particularly rampant in the industrial and manufacturing sectors. …

Source and more information:

https://www.darkreading.com/ics-ot-security/unimicron-presto-attacks-industrial-ransomware-surge

Industrial cybersecurity leadership is evolving from stopping threats to bridging risk, resilience

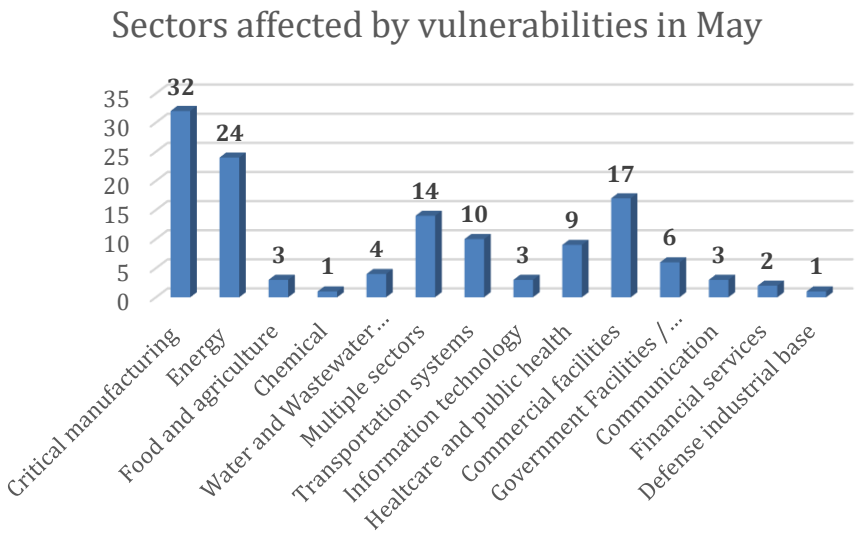
Creating industrial cybersecurity leadership involves fundamentally altering the mindset, one that mirrors the changing nature of the threat landscape and the increasing interdependence between OT (operational technology) and wider business risk. Where once upon a time cybersecurity was a technical matter, siloed from OT infrastructure, modern industrial environments tend to increasingly be digitized and connected, which has brought about the need for new leadership models. …

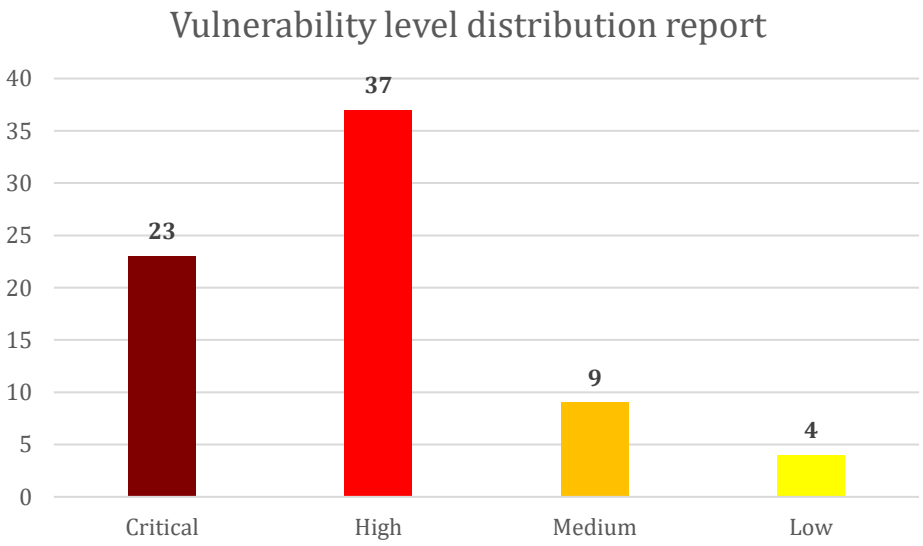
Source and more information:

https://industrialcyber.co/features/industrial-cybersecurity-leadership-is-evolving-from-stopping-threats-to-bridging-risk-resilience/

ICS vulnerabilities

In May 2025, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT and Siemens ProductCERT and Siemens CERT:





ICSA-25-148-01: **Siemens SiPass**

High level vulnerability: Improper Verification of Cryptographic Signature.

Siemens SiPass | CISA

ICSA-25-148-02: **Siemens SiPass Integrated**

High level vulnerability: Out-of-bounds Read.

Siemens SiPass Integrated | CISA

ICSA-25-148-03: **Consilium Safety CS5000 Fire Panel**

Critical level vulnerabilities: Initialization of a Resource with an Insecure Default, Use of Hard-coded Credentials.

Consilium Safety CS5000 Fire Panel | CISA

ICSA-25-148-04: **Instantel Micromate**

Critical level vulnerability: Missing Authentication for Critical Function.

Instantel Micromate | CISA

ICSMA-25-148-01: **Santesoft Sante DICOM Viewer Pro**

High level vulnerability: Out-of-bounds Read.

Santesoft Sante DICOM Viewer Pro | CISA

ICSA-25-146-01: **Johnson Controls iSTAR Configuration Utility (ICU) Tool**

Medium level vulnerability: Use of Uninitialized Variable.

Johnson Controls iSTAR Configuration Utility (ICU) Tool | CISA

ICSA-25-142-01: **Lantronix Device Installer**

Medium level vulnerability: Improper Restriction of XML External Entity Reference.

Lantronix Device Installer | CISA

ICSA-25-142-02: **Rockwell Automation FactoryTalk Historian ThingWorx**

Critical level vulnerability: Improper Restriction of XML External Entity Reference.

Rockwell Automation FactoryTalk Historian ThingWorx | CISA

ICSA-25-140-01: **ABUP IoT Cloud Platform**

Medium level vulnerability: Incorrect Privilege Assignment.

ABUP IoT Cloud Platform | CISA

ICSA-25-140-02: **National Instruments Circuit Design Suite**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Stack-based Buffer Overflow.

National Instruments Circuit Design Suite | CISA

ICSA-25-140-03: **Danfoss AK-SM 8xxA Series**

High level vulnerability: Improper Authentication.

Danfoss AK-SM 8xxA Series | CISA

ICSA-25-140-04: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products**

High level vulnerability: Execution with Unnecessary Privileges.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products | CISA

ICSA-25-140-05: **Siemens Siveillance Video**

Medium level vulnerability: Missing Encryption of Sensitive Data.

Siemens Siveillance Video | CISA

ICSA-25-140-06: **Schneider Electric PrismaSeT Active - Wireless Panel Server**

Critical level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

Schneider Electric PrismaSeT Active - Wireless Panel Server | CISA

ICSA-25-140-07: **Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL**

Critical level vulnerability: Missing Authentication for Critical Function.

Schneider Electric Galaxy VS, Galaxy VL, Galaxy VXL | CISA

ICSA-25-140-08: **Schneider Electric Modicon Controllers**

High level vulnerability: Externally Controlled Reference to a Resource in Another Sphere.

Schneider Electric Modicon Controllers | CISA

ICSA-25-140-09: **AutomationDirect MB-Gateway**

Critical level vulnerability: Missing Authentication For Critical Function.

AutomationDirect MB-Gateway | CISA

ICSA-25-140-10: **Vertiv Liebert RDU101 and UNITY**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Stack-based Buffer Overflow.

Vertiv Liebert RDU101 and UNITY | CISA

ICSA-25-140-11: **Assured Telematics Inc (ATI) Fleet Management System with Geotab Integration**

High level vulnerability: Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Assured Telematics Inc (ATI) Fleet Management System with Geotab Integration | CISA

ICSA-25-037-01: **Schneider Electric EcoStruxure Power Monitoring Expert (PME) (Update B)**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Monitoring Expert (PME) (Update B) | CISA

ICSA-25-023-05: **Schneider Electric EcoStruxure Power Build Rapsody (Update A)**

Low level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

Schneider Electric EcoStruxure Power Build Rapsody (Update A) | CISA

SSA-556937: **VersiCharge AC Series EV Chargers (Update: 1.1.)**

High level vulnerabilities: Missing Immutable Root of Trust in Hardware, Initialization of a Resource with an Insecure Default.

https://cert-portal.siemens.com/productcert/html/ssa-556937.html

SSA-935500: **FTP Server of Nucleus RTOS based APOGEE, TALON and Desigo PXC/PXM Products (Update: 1.3.)**

High level vulnerability: Uncontrolled Resource Consumption.

https://cert-portal.siemens.com/productcert/html/ssa-935500.html

SSA-928984: **Siemens User Management Component (UMC) (Update: 1.2.)**

Critical level vulnerability: Heap-based Buffer Overflow.

https://cert-portal.siemens.com/productcert/html/ssa-928984.html

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.6.)**

Medium level vulnerability: URL Redirection to Untrusted Site ('Open Redirect').

https://cert-portal.siemens.com/productcert/html/ssa-876787.html

SSA-832273: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.9.)**

High level vulnerabilities: Multiple.

https://cert-portal.siemens.com/productcert/html/ssa-832273.html

SSA-819629: **Siemens Industrial Edge Device Kit (Update: 1.2.)**

Critical level vulnerability: Weak Authentication.

https://cert-portal.siemens.com/productcert/html/ssa-819629.html

SSA-770770: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.3.)**

Critical level vulnerabilities: Multiple.

https://cert-portal.siemens.com/productcert/html/ssa-770770.html

SSA-767615: **Siemens SIPROTEC 5 Devices (Update: 1.3.)**

High level vulnerability: Use of Default Credentials.

https://cert-portal.siemens.com/productcert/html/ssa-767615.html

SSA-673996: **Siemens SICAM and SITIPE Products (Update: 1.2.)**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

https://cert-portal.siemens.com/productcert/html/ssa-673996.html

SSA-455250: **Siemens RUGGEDCOM APE1808 Devices Before V11.1.2-h3 (Update: 1.6.)** **High** level vulnerabilities: Multiple.

https://cert-portal.siemens.com/productcert/html/ssa-455250.html

SSA-373591: **Siemens RUGGEDCOM ROS Devices (Update: 1.1.)**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

https://cert-portal.siemens.com/productcert/html/ssa-373591.html

SSA-366067: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.3.)**

Critical level vulnerabilities: Multiple.

https://cert-portal.siemens.com/productcert/html/ssa-366067.html

SSA-354569: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.4.)**

Critical level vulnerabilities: Multiple.

https://cert-portal.siemens.com/productcert/html/ssa-354569.html

SSA-103653: **Siemens Automation License Manager (Update: 1.1.)**

Critical level vulnerability: Integer Overflow or Wraparound.

https://cert-portal.siemens.com/productcert/html/ssa-103653.html

SSA-054046: **Siemens SIMATIC S7-1500 CPUs (Update: 1.5.)**

Medium level vulnerability: Authentication Bypass Using an Alternate Path or Channel.

https://cert-portal.siemens.com/productcert/html/ssa-054046.html

SSA-039007: **Siemens User Management Component (UMC) (Update: 1.5.)**

Critical level vulnerability: Heap-based Buffer Overflow.

https://cert-portal.siemens.com/productcert/html/ssa-039007.html

ICSA-25-135-01: **Siemens RUGGEDCOM APE1808 Devices**

Medium level vulnerability: Insufficiently Protected Credentials, Out-of-bounds Write.

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-25-135-02: **Siemens INTRALOG WMS**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Uncontrolled Resource Consumption, Use After Free, Improper Link Resolution Before File Access ('Link Following'), Improper Input Validation, Inefficient Algorithmic Complexity.

Siemens INTRALOG WMS | CISA

ICSA-25-135-03: **Siemens BACnet ATEC Devices**

High level vulnerability: Improper Input Validation.

Siemens BACnet ATEC Devices | CISA

ICSA-25-135-04: **Siemens Desigo**

High level vulnerability: Missing Authentication for Critical Function.

Siemens Desigo | CISA

ICSA-25-135-05: **Siemens SIPROTEC and SICAM**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Siemens SIPROTEC and SICAM | CISA

ICSA-25-135-06: **Siemens Teamcenter Visualization**

High level vulnerability: Out-of-bounds Read.

Siemens Teamcenter Visualization | CISA

ICSA-25-135-07: **Siemens IPC RS-828A**

Critical level vulnerability: Authentication Bypass by Spoofing.

Siemens IPC RS-828A | CISA

ICSA-25-135-08: **Siemens VersiCharge AC Series EV Chargers**

High level vulnerabilities: Missing Immutable Root of Trust in Hardware, Initialization of a Resource with an Insecure Default.

Siemens VersiCharge AC Series EV Chargers | CISA

ICSA-25-135-09: **Siemens User Management Component (UMC)**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.

Siemens User Management Component (UMC) | CISA

ICSA-25-135-10: **Siemens OZW Web Servers**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Siemens OZW Web Servers | CISA

ICSA-25-135-11: **Siemens Polarion**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Restriction of XML External Entity Reference, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Observable Response Discrepancy.

Siemens Polarion | CISA

ICSA-25-135-12: **Siemens SIMATIC PCS neo**

High level vulnerability: Insufficient Session Expiration.

Siemens SIMATIC PCS neo | CISA

ICSA-25-135-13: **Siemens SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems**

High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Missing Encryption of Sensitive Data, Incorrect Permission Assignment for Critical Resource.

Siemens SIRIUS 3SK2 Safety Relays and 3RK3 Modular Safety Systems | CISA

ICSA-25-135-14: **Siemens APOGEE PXC and TALON TC Series**

Medium level vulnerability: Expected Behavior Violation.

Siemens APOGEE PXC and TALON TC Series | CISA

ICSA-25-135-15: **Siemens Mendix OIDC SSO**

Low level vulnerability: Incorrect Privilege Assignment.

Siemens Mendix OIDC SSO | CISA

ICSA-25-135-16: **Siemens MS/TP Point Pickup Module**

High level vulnerability: Improper Input Validation.

Siemens MS/TP Point Pickup Module | CISA

ICSA-25-135-17: **Siemens RUGGEDCOM ROX II**

Critical level vulnerability: Client-Side Enforcement of Server-Side Security.

Siemens RUGGEDCOM ROX II | CISA

ICSA-25-135-18: **Siemens SCALANCE LPE9403**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Path Traversal: '.../...//', Use of Uninitialized Variable, NULL Pointer Dereference, Out-of-bounds Read, Stack-based Buffer Overflow, Authentication Bypass Using an Alternate Path or Channel, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Cleartext Transmission of Sensitive Information.

Siemens SCALANCE LPE9403 | CISA

ICSA-25-135-19: **ECOVACS DEEBOT Vacuum and Base Station**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Download of Code Without Integrity Check.

ECOVACS DEEBOT Vacuum and Base Station | CISA

ICSA-25-135-20: **Schneider Electric EcoStruxure Power Build Rapsody**

Low level vulnerability: Stack-based Buffer Overflow.

Schneider Electric EcoStruxure Power Build Rapsody | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update C)**

Low level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write.

Mitsubishi Electric Multiple FA Engineering Software Products (Update C) | CISA

ICSA-24-200-01: **Mitsubishi Electric MELSOFT MaiLab and MELSOFT VIXIO (Update A)**

High level vulnerability: Improper Verification of Cryptographic Signature.

Mitsubishi Electric MELSOFT MaiLab and MELSOFT VIXIO (Update A) | CISA

ICSA-25-133-04: **ABB Automation Builder**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

ABB Automation Builder | CISA

ICSA-25-133-03: **Hitachi Energy MACH GWS Products**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Data Query Logic, Improper Limitation of a Pathname to a Restricted Directory, Authentication Bypass by Capture-replay, Missing Authentication for Critical Function.

Hitachi Energy MACH GWS Products | CISA

ICSA-25-133-02: **Hitachi Energy Relion 670/650/SAM600-IO Series**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

Hitachi Energy Relion 670/650/SAM600-IO Series | CISA

ICSA-25-133-01: **Hitachi Energy Service Suite**

Critical level vulnerabilities: Use of Less Trusted Source, Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'), Integer Overflow or Wraparound, Out-of-bounds Write, Allocation of Resources Without Limits or Throttling, Exposure of Sensitive Information to an Unauthorized Actor, Memory Allocation with Excessive Size Value, Out-of-bounds Read, Uncontrolled Resource Consumption, Improper Resource Shutdown or Release, Improper

Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting').

Hitachi Energy Service Suite | CISA

ICSA-25-128-01: **Horner Automation Cscape**

High level vulnerability: Out-of-bounds Read.

Horner Automation Cscape | CISA

ICSA-25-128-02: **Hitachi Energy RTU500 series**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Validation of Specified Index, Position, or Offset in Input.

Hitachi Energy RTU500 Series | CISA

ICSA-25-128-03: **Mitsubishi Electric CC-Link IE TSN**

High level vulnerability: Improper Validation of Specified Quantity in Input.

Mitsubishi Electric CC-Link IE TSN | CISA

ICSA-25-093-01: **Hitachi Energy RTU500 Series (Update A)**

High level vulnerabilities: Null Pointer Dereference, Insufficient Resource Pool, Missing Synchronization.

Hitachi Energy RTU500 Series (Update A) | CISA

ICSMA-25-128-01: **Pixmeo OsiriX MD**

Critical level vulnerabilities: Use After Free, Cleartext Transmission of Sensitive Information.

Pixmeo OsiriX MD | CISA

ICSA-25-126-01: **Optigo Networks ONS NC600**

Critical level vulnerability: Use of Hard-coded Credentials.

Optigo Networks ONS NC600 | CISA

ICSA-25-126-02: **Milesight UG65-868M-EA**

Medium level vulnerability: Improper Access Control for Volatile Memory Containing Boot Code.

Milesight UG65-868M-EA | CISA

ICSA-25-126-03: **BrightSign Players**

High level vulnerability: Execution with Unnecessary Privileges.

BrightSign Players | CISA

ICSA-25-121-01: **KUNBUS GmbH Revolution Pi**

Critical level vulnerabilities: Missing Authentication for Critical Function, Authentication Bypass by Primary Weakness, Improper Neutralization of Server-Side Includes (SSI) Within a Web Page.

KUNBUS GmbH Revolution Pi | CISA

ICSMA-25-121-01: **MicroDicom DICOM Viewer**

High level vulnerabilities: Out-of-Bounds Write, Out-of-Bounds Read.

MicroDicom DICOM Viewer | CISA

The vulnerability reports contain more detailed information, which can be found on the following websites:

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

CISA has published alerts in 2025 May:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-38475 Apache HTTP Server Improper Escaping of Output Vulnerability;
CVE-2023-44221 SonicWall SMA100 Appliances OS Command Injection Vulnerability;
CVE-2025-34028 Commvault Command Center Path Traversal Vulnerability;
CVE-2024-58136 Yiiframework Yii Improper Protection of Alternate Path Vulnerability;
CVE-2025-3248 Langflow Missing Authentication Vulnerability;
CVE-2025-27363 FreeType Out-of-Bounds Write Vulnerability;
CVE-2024-6047 GeoVision Devices OS Command Injection Vulnerability;
CVE-2024-11120 GeoVision Devices OS Command Injection Vulnerability;
CVE-2025-30400 Microsoft Windows DWM Core Library Use-After-Free Vulnerability;
CVE-2025-32701 Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability;
CVE-2025-32706 Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability;
CVE-2025-30397 Microsoft Windows Scripting Engine Type Confusion Vulnerability;
CVE-2025-32709 Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability;
CVE-2025-32756 Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability;
CVE-2024-12987 DrayTek Vigor Routers OS Command Injection Vulnerability;
CVE-2025-4664 Google Chromium Loader Insufficient Policy Enforcement Vulnerability;
CVE-2025-42999 SAP NetWeaver Deserialization Vulnerability;
CVE-2025-4427 Ivanti Endpoint Manager Mobile (EPMM) Authentication Bypass Vulnerability;
CVE-2025-4428 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability;
CVE-2024-11182 MDaemon Email Server Cross-Site Scripting (XSS) Vulnerability;
CVE-2025-27920 Srimax Output Messenger Directory Traversal Vulnerability;
CVE-2024-27443 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting (XSS) Vulnerability;
CVE-2023-38950 ZKTeco BioTime Path Traversal Vulnerability;
Links and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA

Unsophisticated Cyber Actor(s) Targeting Operational Technology

CISA is increasingly aware of unsophisticated cyber actor(s) targeting ICS/SCADA systems within U.S. critical Infrastructure sectors (Oil and Natural Gas), specifically in Energy and Transportation Systems. Although these activities often include basic and elementary intrusion techniques, the presence of poor cyber hygiene and exposed assets can escalate these threats, leading to significant consequences such as defacement, configuration changes, operational disruptions and, in severe cases, physical damage.

Links and more information:

Unsophisticated Cyber Actor(s) Targeting Operational Technology | CISA

Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint advisory to disseminate known tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with threat actors deploying the LummaC2 information stealer (infostealer) malware. LummaC2 malware is able to infiltrate victim computer networks and exfiltrate sensitive information, threatening vulnerable individuals' and organizations' computer networks across multiple U.S. critical infrastructure sectors. According to FBI information and trusted third-party reporting, this activity has been observed as recently as May 2025. The IOCs included in this advisory were associated with LummaC2 malware infections from November 2023 through May 2025.

Links and more information:

Threat Actors Deploy LummaC2 Malware to Exfiltrate Sensitive Data from Organizations | CISA

Guidance for SIEM and SOAR Implementation

CISA, in collaboration with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and other international and U.S. partners, released guidance for organizations seeking to procure Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.

Links and more information:

Guidance for SIEM and SOAR Implementation | CISA

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in June 2025:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Industrial Control Systems Cybersecurity (Virtual)(ICS300)
- Industrial Control Systems Evaluation (Virtual)(401V)
- ICS Cybersecurity & RED-BLUE Exercise (In-Person)(ICS301)
- Industrial Control Systems Evaluation (In-Person)(401L)
- Introduction to Control Systems Cybersecurity (In-Person)(101)
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- ICS/SCADA Cyber Security
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

- Industrial Control System (ICS) & SCADA Cyber Security Training

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

- ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

- ICS/OT Cyber ICS/OT Cybersecurity as per NIST 800-82 Updated - Part1

https://www.udemy.com/course/ics-cybersecurity/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

https://www.infosectrain.com/operational-technology-ot-training-courses/#courses

- OT Railway Cybersecurity (OTCS)

https://informaconnect.com/ot-railway-cybersecurity-otcs/

- OT Security Expert (*Master OT/ICS security essentials for protecting critical infrastructure in the digital era*)

https://opswatacademy.com/courses/ot-security-expert

- CTR-008 - OT-Security Awareness E-Learning Course

https://www.yokogawa.com/eu/solutions/products-and-services/trainings-und-workshops/kompetenztrainings/ctr-008-ot-security-awareness-e-learning-course/

- Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards

Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards | EC-Council Learning

ICS podcasts

People listen more and more podcasts nowadays. Whether it's for our personal interests or for our professional development, the world of podcasts is a great possibility to be well informed. In this section, we bring together the ICS security podcasts from the previous month.

Dale Peterson

This podcast is named after and made by one of the most famous ICS security expert, Dale Peterson. It's made on Wednesdays on every week and the usual structure contains an opening monologue, interviews with guests and listener questions on topics that are on the leading, or even bleeding edge of OT and ICS security. The podcast is also interactive, so the listeners could ask question from Dale and the guests.

You can find all of Peterson's podcasts on the below URL.

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

This podcast is discussing major industrial cybersecurity topics and features industry experts covering everything from ransomware through critical infrastructure to supply chain attacks. Tune in to stay on top of the latest cybersecurity trends, threats and tactics. Hosted by Gary Cohen and Tyler Wall.

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

BEERISAC: OT/ICS Security Podcast Playlist

A curated playlist of Operational Technology and ICS Cyber Security related podcast episodes by ICS Security enthusiasts.

At this link, you can find numerous podcasts on the topic of ICS (Industrial Control Systems) created by various content producers. It's worth browsing through and listening to podcasts that are of interest to the organization or the readers of this newsletter themselves.

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/