BLACK CELL
Protecting critical infrastructures

Industrial Control Systems security feed

2026 January

2026 January, 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

1. ICS good practices, recommendations

Strengthening Operational Technology Resilience: Nine Considerations

Establishing robust network segmentation only scratches the surface of safeguarding operational technology (OT) environments. Enhancing security and resilience further requires implementing focused strategies such as advanced monitoring, comprehensive documentation and OT-specific incident response plans.

As cybersecurity teams increasingly oversee OT and industrial control systems (ICS), aligning priorities and resources is critical. OT environments are diverse, spanning industries like manufacturing, healthcare and utilities. Whether it's factory automation or building access control, safeguarding OT cyber-physical systems has become vital. According to KnowBe4, cyberattacks targeting critical OT environments are expected to increase by 30% annually, highlighting the urgency of prioritizing OT security. Achieving true resilience demands more extensive efforts. Below are nine considerations for organizations beginning discussions around OT security and resilience. For best practices for various stakeholder groups, you may refer to the ISA/IEC 62443 series of standards for automation and control systems cybersecurity.

1. Assemble a Cross-Functional Team
2. Diagram and Document OT Systems
3. Maintain Dynamic Asset Inventories
4. Enhance Logging and Alerting
5. Eliminate Shared IT/OT Accounts
6. Segment Within OT Networks
7. Adopt Risk-Based Vulnerability Management
8. Develop an OT-Specific Incident Response Plan (IRP)
9. Invest in Continued Education

Some Final Thoughts to Leave You With...

IT-centric assumptions often lead to flawed strategies for OT environments. Basic IT practices, such as automated password lockouts, may not translate safely to OT. A collaborative cross-functional team can mitigate these missteps, ensuring tailored solutions that respect the nuances of OT systems. As you embark on enhancing OT resilience, the considerations above may be helpful in starting discussions. Recognize that IT and OT are distinct domains requiring customized security measures, and refer to established OT cybersecurity frameworks for guidance. By laying a solid foundation, organizations can mitigate risks to their OT environments, safeguarding operations and achieving long-term resilience.

Source and links and more information:

https://gca.isa.org/blog/strengthening-operational-technology-resilience-nine-considerations

2. ICS conferences

In February 2026, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

DistribuTECH International 2026

From cutting-edge solutions in grid automation, energy efficiency, and demand response to breakthroughs in DER management, smart cities, transportation electrification, and cybersecurity, DTECH® delivers the insights and connections that move the industry forward. Whether you're focused on resiliency, reliability, sustainability, or grid modernization, DTECH® events offer unmatched value, collaboration, and opportunities to spark real transformation - today and tomorrow. Join and be part of the momentum shaping the future of transmission and distribution.

San Diego, CA, USA; 2nd – 5th February 2026

More details can be found on the following website:

https://www.distributech.com/?utm_source=iiotworld

How AI Is Driving the Future of Industrial Operations and Supply Chain

Are you ready to explore the cutting-edge advancements in Industrial AI? Join us at the ARC Forum, where industry leaders and innovators come together to discuss the transformative power of AI in various sectors. This year's forum kicks off with a keynote and executive panel discussion on the latest trends and applications of Industrial AI. What's real and what's hype? What have leaders struggled with?

Join to learn more about:

- Smart Manufacturing and Digital
- Transformation
- Robotics
- Industrial Data Fabrics
- AI and Supply Chain
- Data Centers, AI, and Energy and more…

Orlando, FL, USA; 9th – 12th February 2026

More details can be found on the following website:

https://www.arcweb.com/events/arc-industry-leadership-forum-orlando

S4X26

Set free a conservative, slow moving, change resistant community to discover new ideas and come up with innovative ways to use these new ideas to deploy secure, resilient and better ICS. It's 3-days on 3-stages of sessions for the advanced OT security pro and early adopters. S4 is much more than the sessions. You will be with 1,000+ of the best in world talent. Influencers. Creators. People who are pushing boundaries. And we have a lot of fun with parties and eclectic experiences. All this in a creative environment that is designed to break you out of your normal thought patterns.

The best way to understand how S4 is different is to come to the event. The second best way is to ask someone who has attended, obviously we are biased. S4 is not for everyone. If you are an early adopter, like to be on the leading edge, or enjoy hearing, considering and creating new ideas, then there is a good chance S4 will be a great event for you.

Miami South Beach, FL, USA; 23rd – 26th February 2026

More details can be found on the following website:

https://s4xevents.com/?utm_source=iiot-world.com

ManuSec

European manufacturers are grappling with a surge in cyber and ransomware attacks, with increasingly sophisticated threat actors disrupting operations and compromising sensitive data across diverse sectors. Last year, European manufacturers experienced 90% more data breaches over the last year, with 71% of companies now considering cybersecurity as a high priority.

As factories adopt smarter, more connected systems, they are becoming prime targets. Consequently, this edition of ManuSec Europe will focus on "Securing Our Manufacturers Today To Shape the Future of OT Cyber Security". Manufacturers face issues through integrating legacy systems with new digital tools, high upfront costs for their cyber programmes, and shortages in skilled labour needed to manage advanced technologies. Hence, the agenda this year will comprehensively explore both the largest issues of today to ensure our manufacturing operations stay secure tomorrow.

Munchen, Germany; 26th – 27th February 2026

More details can be found on the following website: https://europe.manusecevent.com/

3. ICS incidents

Romanian water authority, energy producer hit by cyber attacks in apparent coordinated holiday campaign

In December 2025, Romania experienced two closely timed cyber incidents affecting its national water management authority, Administrația Națională "Apele Române", and its largest coal-based power producer, Oltenia Energy Complex. While neither attack directly disrupted industrial control systems (ICS), both incidents underscore the growing OT risk arising from compromised IT environments that support critical infrastructure operations.

The attack on Romanian Waters affected approximately 1,000 IT systems, including servers, workstations, email, DNS, and web services. Attackers encrypted data using Windows BitLocker, disabling administrative and coordination capabilities. Although water flows, dams, and field-level control systems reportedly remained operational, the loss of central IT systems significantly reduced operational visibility, coordination, and incident response capacity, all of which are critical for safe OT operation during abnormal conditions.

Shortly thereafter, Oltenia Energy Complex detected a ransomware attack attributed to the Gentlemen threat group. Core enterprise systems (ERP), document management, email, and the company website were encrypted and taken offline. While electricity generation and the National Energy System were not directly impacted, the attack impaired the business and planning systems that underpin fuel logistics, maintenance scheduling, and workforce coordination, creating latent risks for OT continuity and resilience.

From an OT security perspective, both attacks followed a similar strategic pattern: target the IT layer that enables industrial operations rather than the control systems themselves. This approach allows attackers to degrade industrial resilience, delay decision-making, and increase the likelihood of operational errors without triggering immediate safety shutdowns or detection by OT monitoring tools.

The timing of the attacks, during the end-of-year holiday period further amplified OT risk by exploiting reduced staffing and slower escalation paths. Additionally, the dependency between water management and energy production highlights a broader systemic concern: compromise of upstream infrastructure can indirectly affect downstream industrial operations, even when OT networks remain segmented.

These incidents reinforce the need for stronger IT–OT integration controls, robust identity and access management, tested manual fallback procedures, and heightened OT readiness during high-risk periods. They demonstrate that modern threats to industrial environments increasingly materialize through IT compromise, with OT impact emerging as a second-order effect rather than a direct attack vector.

The source is available at the following link:

https://industrialcyber.co/critical-infrastructure/romanian-water-authority-energy-producer-hit-by-cyber-attacks-in-apparent-coordinated-holiday-campaign/

Sandworm Blamed for Wiper Attack on Poland Power Grid

In December, Poland's energy sector was targeted in a destructive cyberattack that has been attributed to Russia-linked threat actors, specifically the Sandworm advanced persistent threat (APT) group. The attack, which occurred on December 29–30, targeted two combined heat and power plants as well as a system used to manage electricity generated from renewable energy sources such as wind and photovoltaic installations. According to Polish authorities, the attack was one of the most serious cyber incidents the country's energy infrastructure had faced in recent years. However, it ultimately failed to cause operational disruption: no blackout or other service outage occurred.

Although Poland's Prime Minister did not officially name the threat actor at the time of the announcement, responsibility was publicly associated with Russia. Subsequent technical analysis by cybersecurity company ESET attributed the operation to the Sandworm group with medium confidence. ESET reported strong similarities between this incident and previous Sandworm campaigns, based on the malware used and the attackers' tactics, techniques, and procedures (TTPs). The malware deployed in the Polish incident was a previously undocumented data-wiping tool, which ESET named DynoWiper (detected as Win32/KillFiles.NMO). As with other Sandworm wiper operations, the intent appeared to be destructive rather than espionage-driven.

Sandworm has a long track record of disruptive cyber operations, particularly against critical infrastructure. The group was responsible for the 2015 BlackEnergy attack on Ukraine's power grid, which caused power outages affecting hundreds of thousands of people, and for the 2017 NotPetya attack, a globally impactful wiper masquerading as ransomware. The timing of the Polish attack - roughly the 10th anniversary of the BlackEnergy incident - was noted by researchers as symbolically significant.

Since Russia's full-scale invasion of Ukraine in 2022, Sandworm activity has intensified, with repeated wiper attacks against Ukrainian government, energy, logistics, and agricultural organizations. These campaigns are widely viewed as aligned with Russian geopolitical and military objectives, aiming to disrupt essential services and weaken economic resilience. Poland's status as a NATO member and key supporter of Ukraine likely increases its exposure to such state-aligned cyber operations. Overall, the incident highlights the continued risk of destructive cyberattacks against European critical infrastructure, even when defensive measures prevent immediate operational impact.

The source is available at the following link:

https://www.darkreading.com/threat-intelligence/sandworm-wiper-attack-poland-power-grid

4. Book recommendation

Fundamentals of Industrial Security

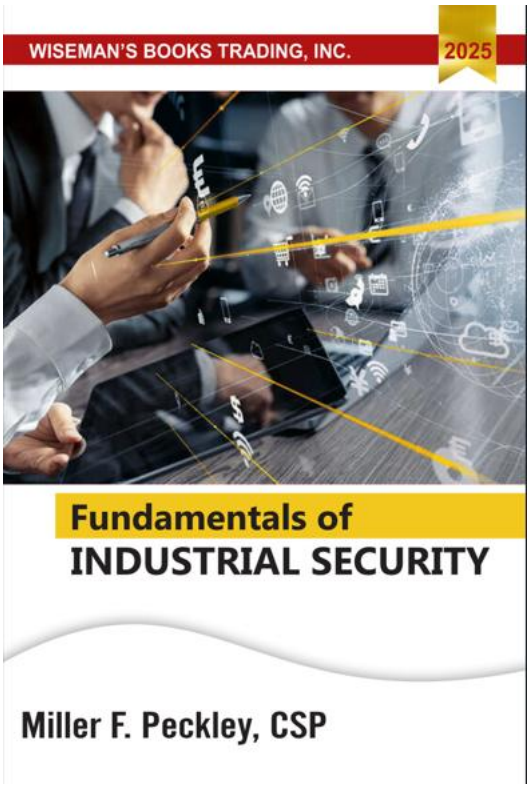
This book, Fundamentals of Industrial Security, is a first-year subject for students taking a Bachelor of Science in Industrial Security Management course. It covers the basic, fundamentals, and foundational principles of security in general and Industrial Security to be specific. This humble piece of work labored with love and passion can also be used as a reference by students taking the course Bachelor of Science in Criminology enrolled in a subject Introduction to "Industrial Security Concepts," additional review materials for Criminology graduates preparing for Criminologists Licensure Examination, and guide reference for professionals in the practice of the Security Profession.

Author/Editor: Miller F. Peckley

Year of issue: 2025

The book is available at the following link:

https://www.wisemansbookstrading.com/product/fundamentals-of-industrial-security/



5. ICS security news selection

Important articles dealing with critical infrastructure protection and industrial cybersecurity in January:

1. **Scattered Lapsus$ resurfaces with brokered access model, raising risks for industrial and critical infrastructure**
2. **Threats to Critical Infrastructure Expected to Intensify**
3. **Global Cyber Agencies Issue AI Security Guidance for Critical Infrastructure OT**
4. **Rethinking OT security for project heavy shipyards**
5. **Industrial cyber governance hits inflection point, shifts toward measurable resilience and executive accountability**
6. **Spanish energy giant Endesa discloses data breach affecting customers**
7. **Cyberthreats Target Legacy Systems in Manufacturing**
8. **Firmware Trust: A Blind Spot in OT**
9. **Aligning OT cybersecurity with uptime, safety, and throughput as digital transformation reshapes industrial risk**
10. **New Reports Reinforce Cyberattack's Role in Maduro Capture Blackout**
11. **Key Areas of Convergence for IT-OT Security in Energy Sector**
12. **MITRE Launches New Security Framework for Embedded Systems**
13. **CISA publishes initial list of hardware and software categories supporting post-quantum cryptography to guide adoption**
14. **Russian Sandworm Hackers Blamed for Cyberattack on Polish Power Grid**
15. **Indurex Emerges From Stealth to Close Security Gap in Cyber-Physical Systems**

Scattered Lapsus$ resurfaces with brokered access model, raising risks for industrial and critical infrastructure

New Cyfirma research flagged the resurgence of the Scattered Lapsus$ collective, with monitoring of underground forums and Telegram channels indicating the group is rebuilding capacity for large-scale intrusion and extortion campaigns. Analysts say the actors are actively recruiting initial access brokers, insider collaborators, and sellers of corporate credentials, while signaling a more structured operating model that could significantly expand their ability to compromise major enterprises.

Early indicators mark a shift toward high-revenue enterprises with annual turnover exceeding US$500 million, spanning telecommunications, software and gaming supply chains, BPO and call-center environments, and cloud and hosting providers, with operations focused on

networks in the U.S., Australia, the U.K., Canada, and France. The group also operates structured commission tiers, offering 25% for access to any Active Directory-joined system and 10% for credentials tied to platforms such as Okta, the Azure portal, or AWS IAM root accounts. …

Source and more information:

https://industrialcyber.co/ransomware/scattered-lapsus-resurfaces-with-brokered-access-model-raising-risks-for-industrial-and-critical-infrastructure/

Threats to Critical Infrastructure Expected to Intensify

Attacks against critical infrastructure are expected to increase in scope and intensity including hacks on operational technology systems. State actors are now looking for ways to cause damage and disrupt operations, rather than simply steal secrets, according to cybersecurity experts.

ISMG's Tony Morbin compiled perspectives of defense leaders, cybersecurity practitioners, technology vendors and analysts to analyze the threats to critical infrastructure and what the future holds for enterprise security across multiple domains. Most predict that future attacks will follow geopolitical conflicts and continue to play a role in kinetic warfare. …

Source and more information:

https://www.ot.today/threats-to-critical-infrastructure-expected-to-intensify-a-30456

Global Cyber Agencies Issue AI Security Guidance for Critical Infrastructure OT

The guidance, published on the website of the cybersecurity agency CISA, was authored by government organizations in the United States, the United Kingdom, Canada, Germany, the Netherlands, and New Zealand.

Integrating AI with industrial control systems (ICS) and other OT can have significant benefits. The agencies have provided several examples of use cases.

For instance, in the case of field devices such as sensors and actuators, the data they generate can be used to train AI models and identify significant deviations. In the case of programmable logic controllers (PLCs) and remote terminal units (RTUs), AI can be leveraged for classifying load balancing and anomaly detection. …

Source and more information:

https://www.securityweek.com/global-cyber-agencies-issue-ai-security-guidance-for-critical-infrastructure-ot/

Rethinking OT security for project heavy shipyards

In this Help Net Security interview, Hans Quivooij, CISO at Damen Shipyards Group, discusses securing OT and ICS in the shipyard. He outlines how project-based operations, rotating contractors, and temporary systems expand the threat surface and complicate access control.

Quivooij also covers visibility in legacy environments and the risks introduced by IT and OT integration.

Shipyards blend long-lived industrial equipment with short-lived projects and contractors. How does that project-based operating model change the threat surface compared to more static OT environments? …

Source and more information:

https://www.helpnetsecurity.com/2026/01/12/hans-quivooij-damen-shipyards-group-securing-shipyard-ot-ics/

Industrial cyber governance hits inflection point, shifts toward measurable resilience and executive accountability

Industrial cyber governance is at a tipping point as legacy models have largely been unable to keep pace with converging IT, OT, cloud, and AI-driven control systems. Treating cybersecurity as a compliance discipline is an impractical approach anymore in a world where cyber incidents lead to safety incidents, production loss, and a rolling supply chain disruption. IBM's 2024 Cost of a Data Breach Report highlights breaches involving critical infrastructure as some of the most costly, further highlighting the importance of governance models that anticipate operational risk, rather than audit readiness. …

Source and more information:

https://industrialcyber.co/features/industrial-cyber-governance-hits-inflection-point-shifts-toward-measurable-resilience-and-executive-accountability/

Spanish energy giant Endesa discloses data breach affecting customers

Spanish energy provider Endesa and its Energía XXI operator are notifying customers that hackers accessed the company's systems and accessed contract-related information, which includes personal details.

Endesa is the largest electric utility company in Spain, now owned by Enel Group, that distributes gas and electricity to more than 10 million customers in Spain and Portugal. In total, the company says it has about 22 million clients.

The energy company notified its Energía XXI affected customers affected by the breach and also disclosed the security incident publicly, saying that it detected unauthorized access to its commercial platform. …

Source and more information:

https://www.bleepingcomputer.com/news/security/spanish-energy-giant-endesa-discloses-data-breach-affecting-customers/

Cyberthreats Target Legacy Systems in Manufacturing

Legacy OT systems now face heightened exposure as manufacturers accelerate digital transformation. With ransomware attacks up nearly 90% year-over-year, cybersecurity leaders warn that "silver bullet" solutions fall short. Operational resilience must be built on a foundation of diverse tools, human readiness and cross-functional coordination.

ManuSec Europe 2026 brings together CISOs, security practitioners and strategists to explore pragmatic steps manufacturers can take today, including compensating controls, IT and OT cross-training between teams, and building a culture of ownership over rigid incident playbooks. Overly centralized programs and tool uniformity only compound vulnerabilities in high-utilization environments, according to a panel of conference speakers. …

Source and more information:

https://www.ot.today/cyberthreats-target-legacy-systems-in-manufacturing-a-30497

Firmware Trust: A Blind Spot in OT

Hardware still operates as a trusted black box in many OT environments, even as attackers shift focus to embedded software and firmware. CISOs must rethink how trust gets established and maintained in these devices, said Brahman Thiyagalingham, CISO at GME.

"At a very minimum, I would expect some mechanism to detect whether firmware has been tampered with from the manufacturer's published version," Thiyagalingham said. "If malware can attack firmware, you need to know whether it has changed in any way." …

Source and more information:

https://www.ot.today/firmware-trust-blind-spot-in-ot-a-30506

Aligning OT cybersecurity with uptime, safety, and throughput as digital transformation reshapes industrial risk

Industrial cybersecurity is standing at a crossroads where 'locking down the perimeter' is no longer enough to protect increasingly interconnected factories, grids, and process environments. Traditional defenses fall short when IT networks are connected to OT systems and attackers leverage this broadened attack surface to cause production interruptions, safety degradation, and negate reliability improvements that took years to develop within a matter of a few minutes. More than one-third of manufacturers identify enhancing IT/OT security as a key business priority, and nearly half say they intend to validate uptime and quality using real-time analytics and AI, rather than just relying on these technologies to identify breaches. …

Source and more information:

https://industrialcyber.co/features/aligning-ot-cybersecurity-with-uptime-safety-and-throughput-as-digital-transformation-reshapes-industrial-risk/

New Reports Reinforce Cyberattack's Role in Maduro Capture Blackout

US officials briefed on the January 3 extraction of Venezuelan President Nicolas Maduro say the operation leveraged cyberattacks to trigger power outages and disable air defense radars, according to The New York Times.

Shortly after the world learned of Maduro's capture, US President Donald Trump stated that "the lights of Caracas were largely turned off due to a certain expertise that we have".

While Trump didn't explicitly mention a cyberattack, his comments were widely seen that way.

Robert Lee, CEO of industrial cybersecurity firm Dragos, noted at the time that from a technical standpoint the US could have caused a power outage and disrupted air defenses using a cyberattack on operational technology (OT) systems. …

Source and more information:

https://www.securityweek.com/new-reports-reinforce-cyberattacks-role-in-maduro-capture-blackout/

Key Areas of Convergence for IT-OT Security in Energy Sector

The energy sector is undergoing rapid digital transformation to meet demands to power data centers, expand generation of renewable energy and modernize distribution. New connected systems that support distributed grid architectures are driving the need for convergence of IT systems and operational technologies, widening the threat landscape for cyber and kinetic attacks that cause widespread damage. …

Source and more information:

https://www.ot.today/key-areas-convergence-for-it-ot-security-in-energy-sector-a-30485

MITRE Launches New Security Framework for Embedded Systems

MITRE on Tuesday announced the launch of Embedded Systems Threat Matrix (ESTM), a cybersecurity framework designed to help organizations protect critical embedded systems.

Inspired by the popular ATT&CK framework and derived from MITRE's theoretical research and proof-of-concept models, the ESTM categorizes specific attack tactics and techniques tailored to hardware and firmware environments.

The model maps both established and emerging attack vectors to assist organizations in identifying vulnerabilities within embedded architectures. …

Source and more information:

https://www.securityweek.com/mitre-launches-new-security-framework-for-embedded-systems/

CISA publishes initial list of hardware and software categories supporting post-quantum cryptography to guide adoption

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an initial list of hardware and software categories that currently support, or are expected to support, post-quantum cryptography (PQC) standards. The list helps organizations plan PQC migration strategies and evaluate future technology investments in an evolving cybersecurity landscape. It includes examples of widely available products within these categories that use PQC standards to protect sensitive information. …

Source and more information:

https://industrialcyber.co/cisa/cisa-publishes-initial-list-of-hardware-and-software-categories-supporting-post-quantum-cryptography-to-guide-adoption/

Russian Sandworm Hackers Blamed for Cyberattack on Polish Power Grid

The Russian state-sponsored APT named Sandworm was behind the December 2025 cyberattack targeting Poland's power grid, cybersecurity firm ESET reports.

Poland's energy infrastructure, including two combined heat and power (CHP) plants and a renewable energy management system, was targeted by hackers on December 29-30, and Polish officials blamed Russia for the assault.

Said to have been the largest cyberattack against Poland in years, the December 2025 incident was thwarted before it could cause a blackout or compromise critical infrastructure, the country's officials said earlier this month. …

Source and more information:

https://www.securityweek.com/russian-sandworm-hackers-blamed-for-cyberattack-on-polish-power-grid/

Indurex Emerges From Stealth to Close Security Gap in Cyber-Physical Systems

AI security OT

Indurex, a Netherlands-based cybersecurity startup that specializes in protecting cyber-physical systems, emerged from stealth mode on Tuesday.

The company has developed a solution that leverages AI and data collected from OT and IT systems to provide organizations with the resources needed to protect critical infrastructure, manufacturing, and industrial operations.

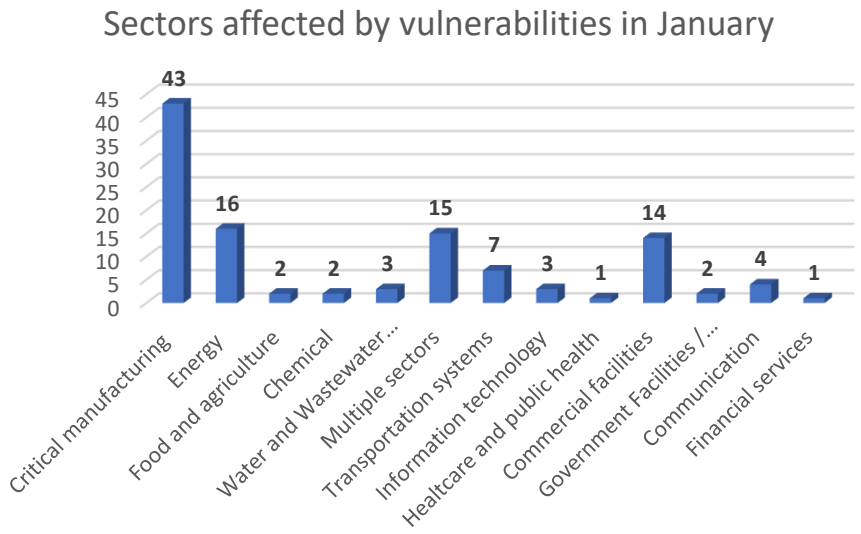
Indurex was founded by Jalal Bouhdada, who serves as the company's CEO, and Maarten Oosterink, who serves as COO. …

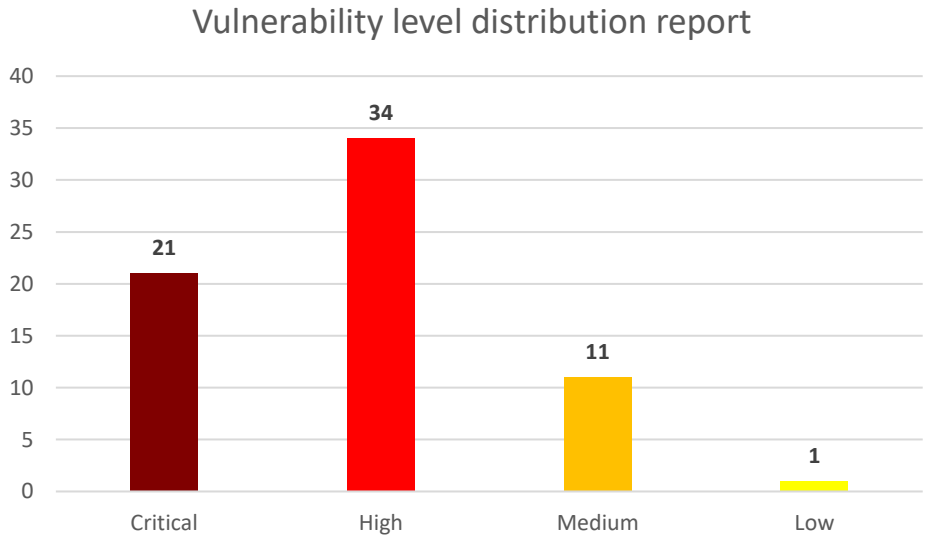
Source and more information:

https://www.securityweek.com/indurex-emerges-from-stealth-to-close-security-gap-in-cyber-physical-systems/

6. ICS vulnerabilities

In January 2026, 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-26-029-01: **KiloView Encoder Series**

Critical level vulnerability: Missing Authentication for Critical Function.

KiloView Encoder Series | CISA

ICSA-26-029-02: **Rockwell Automation ArmorStart LT**

High level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation ArmorStart LT | CISA

ICSA-26-029-03: **Rockwell Automation ControlLogix**

High level vulnerability: Missing Release of Memory after Effective Lifetime.

Rockwell Automation ControlLogix | CISA

ICSA-25-126-03: **BrightSign Players (Update A)**

High level vulnerabilities: Execution with Unnecessary Privileges, Use of Default Credentials.

BrightSign Players (Update A) | CISA

ICSA-25-140-04: **Mitsubishi Electric Iconics Digital Solutions / Mitsubishi Electric GENESIS64 (Update D)**

Medium level vulnerability: Execution with Unnecessary Privileges.

Mitsubishi Electric Iconics Digital Solutions / Mitsubishi Electric GENESIS64 (Update D) | CISA

ICSA-25-205-01: **Mitsubishi Electric CNC Series (Update B)**

High level vulnerability: Uncontrolled Search Path Element.

Mitsubishi Electric CNC Series (Update B) | CISA

ICSA-26-027-01: **iba Systems ibaPDA**

Critical level vulnerability: Incorrect Permission Assignment for Critical Resource.

iba Systems ibaPDA | CISA

ICSA-26-027-02: **Festo Didactic SE MES PC**

Critical level vulnerabilities: Buffer Over-read, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Input Validation, Improper Handling of Values, Uncontrolled Resource Consumption, Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), Double Free, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Use After Free, Exposure of Sensitive Information to an Unauthorized Actor, Out-of-bounds Read, Improper Null Termination, Incorrect Calculation of Buffer Size, Path Traversal: '../filedir', Reachable Assertion, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Use of Password Hash With Insufficient Computational Effort, Out-of-bounds Write, Incorrect Privilege Assignment, Improper Control of Generation of Code ('Code Injection'), Improper Authentication, Stack-based Buffer Overflow, NULL Pointer Dereference, Missing Initialization of Resource, Null Byte Interaction

Error (Poison Null Byte), Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Preservation of Permissions, Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'), Integer Overflow or Wraparound, Uncontrolled Recursion, URL Redirection to Untrusted Site ('Open Redirect'), Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting'), Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Free of Memory not on the Heap, Use of Uninitialized Resource, Improper Handling of Invalid Use of Special Elements, Improper Use of Validation Framework.

Festo Didactic SE MES PC | CISA

ICSA-26-027-03: **Schneider Electric Zigbee Products**

Medium level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Uncontrolled Resource Consumption.

Schneider Electric Zigbee Products | CISA

ICSA-26-027-04: **Johnson Controls Products**

Critical level vulnerability: Improper Neutralization of Special Elements used in a Command ('Command Injection').

Johnson Controls Products | CISA

ICSA-26-022-01: **Schneider Electric EcoStruxure Process Expert**

High level vulnerability: Incorrect Default Permissions.

Schneider Electric EcoStruxure Process Expert | CISA

ICSA-26-022-02: **AutomationDirect CLICK Programmable Logic Controller**

Medium level vulnerabilities: Weak Encoding for Password, Plaintext Storage of a Password.

AutomationDirect CLICK Programmable Logic Controller | CISA

ICSA-26-022-03: **Rockwell Automation CompactLogix 5370**

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

Rockwell Automation CompactLogix 5370 | CISA

ICSA-26-022-04: **Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool**

High level vulnerability: Stack-based Buffer Overflow.

Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool | CISA

ICSA-26-022-05: **Weintek cMT X Series HMI EasyWeb Service**

High level vulnerabilities: External Control of Assumed-Immutable Web Parameter, Unverified Password Change.

Weintek cMT X Series HMI EasyWeb Service | CISA

ICSA-26-022-06: **Hubitat Elevation Hubs**

Critical level vulnerability: Authorization Bypass Through User-Controlled Key.

Hubitat Elevation Hubs | CISA

ICSA-26-022-07: **Delta Electronics DIAView**

High level vulnerability: Improper Neutralization of Special Elements used in a Command ('Command Injection').

Delta Electronics DIAView | CISA

ICSA-26-022-08: **EVMAPA**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration.

EVMAPA | CISA

ICSA-25-352-08: **Axis Communications Camera Station Pro, Camera Station, and Device Manager (Update B)**

Critical level vulnerabilities: Deserialization of Untrusted Data, Improper Certificate Validation, Authentication Bypass Using an Alternate Path or Channel.

Axis Communications Camera Station Pro, Camera Station, and Device Manager (Update B) | CISA

ICSA-25-184-01: **Hitachi Energy Relion 670/650 and SAM600-IO Series (Update B)**

Medium level vulnerability: Improper Check for Unusual or Exceptional Conditions.

Hitachi Energy Relion 670/650 and SAM600-IO Series (Update B) | CISA

ICSA-26-020-01: **Schneider Electric EcoStruxure Foxboro DCS**

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.

Schneider Electric EcoStruxure Foxboro DCS | CISA

ICSA-26-020-02: **Schneider Electric devices using CODESYS Runtime**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Validation of Integrity Check Value, Improper Validation of Consistency within Input, Out-of-bounds Write, Stack-based Buffer Overflow, Untrusted Pointer Dereference, Improper Input Validation, Files or Directories Accessible to External Parties, Uncontrolled Search Path Element, Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Improper Restriction of Excessive Authentication Attempts, Exposure of Resource to Wrong Sphere.

Schneider Electric devices using CODESYS Runtime | CISA

ICSA-26-020-03: **Rockwell Automation Verve Asset Manager**

High level vulnerabilities: Insecure Storage of Sensitive Information, Cleartext Storage of Sensitive Information.

Rockwell Automation Verve Asset Manager | CISA

ICSA-24-326-04: **Schneider Electric Modicon M340, MC80, and Momentum Unity M1E (Update B)**

High level vulnerabilities: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Schneider Electric Modicon M340, MC80, and Momentum Unity M1E (Update B) | CISA

ICSA-25-070-01: **Schneider Electric Uni-Telway Driver (Update B)**

Medium level vulnerability: Improper Input Validation.

Schneider Electric Uni-Telway Driver (Update B) | CISA

ICSA-25-184-03: **Mitsubishi Electric MELSOFT Update Manager (Update A)**

High level vulnerabilities: Integer Underflow (Wrap or Wraparound), Protection Mechanism Failure.

Mitsubishi Electric MELSOFT Update Manager (Update A) | CISA

SSA-978177: **Vulnerability in Nozomi Guardian/CMC Before 25.4.0 on RUGGEDCOM APE1808 Devices (Update: 1.3.)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Execution with Unnecessary Privileges, Incorrect Authorization, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

SSA-978177

SSA-928984: **Heap-based Buffer Overflow Vulnerability in User Management Component (UMC) (Update: 1.4.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-928984

SSA-912274: **Multiple Vulnerabilities in RUGGEDCOM ROX Before V2.17 (Update: 1.1.)**

High level vulnerabilities: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Neutralization of Special Elements used in a Command ('Command Injection').

SSA-912274

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.5.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-858251: **Authentication Bypass Vulnerabilities in OPC UA (Update: 1.2.)**

Critical level vulnerabilities: Observable Timing Discrepancy, Authentication Bypass by Primary Weakness.

SSA-858251

SSA-832273: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.3 on RUGGEDCOM APE1808 Devices (Update: 2.1.)**

High level vulnerabilities: Multiple.

SSA-832273

SSA-698820: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.4 on RUGGEDCOM APE1808 Devices (Update: 2.0.)**

High level vulnerabilities: Stack-based Buffer Overflow, Session Fixation, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Check for Unusual or Exceptional Conditions, Missing Authentication for Critical Function, Incorrect Parsing of Numbers with Different Radices, Improperly Implemented Security Check for Standard, Improper Access Control, Insertion of Sensitive Information into Log File, Channel Accessible by Non-Endpoint, Buffer Over-read.

SSA-698820

SSA-693776: **Multiple Vulnerabilities in Industrial Communication Devices based on SINEC OS before V3.2 (Update: 1.1.)**

High level vulnerabilities: Incorrect Authorization, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

SSA-693776

SSA-366067: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.1 on RUGGEDCOM APE1808 Devices (Update: 1.7.)**

Critical level vulnerabilities: Multiple.

SSA-366067

SSA-365200: **Google Chrome Type Confusion Vulnerability in Siemens Products (Update: 1.1.)**

High level vulnerability: Access of Resource Using Incompatible Type ('Type Confusion').

SSA-365200

SSA-364175: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update: 1.7.)**

Critical level vulnerabilities: Truncation of Security-relevant Information, Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Improper Input Validation, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Out-of-bounds Write, Uncontrolled Resource Consumption, Improper Neutralization of Special Elements used in a Command ('Command Injection'), Improper Check for Unusual or Exceptional Conditions.

SSA-364175

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 1.5.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-212953: **Multiple Vulnerabilities in COMOS (Update: 1.1.)**

Critical level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Input Validation, Generation of Predictable Numbers or Identifiers, mproper Certificate Validation.

SSA-212953

SSA-201595: **Privilege Escalation Vulnerability in WIBU CodeMeter Runtime Affecting the Desigo CC Product Family and SENTRON Powermanager (Update: 1.2.)** **High** level vulnerability: Least Privilege Violation.

SSA-201595

SSA-082556: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1.5 (Update: 1.2.)**

High level vulnerabilities: Multiple.

SSA-082556

ICSA-26-015-01: **AVEVA Process Optimization**

Critical level vulnerabilities: Improper Control of Generation of Code ('Code Injection'), Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Uncontrolled Search Path Element, Missing Authorization, Use of Potentially Dangerous Function, Cleartext Transmission of Sensitive Information.

AVEVA Process Optimization | CISA

ICSA-26-015-02: **Festo Firmware**

Critical level vulnerability: Insufficient Technical Documentation.

Festo Firmware | CISA

ICSA-26-015-03: **Siemens TeleControl Server Basic**

High level vulnerability: Execution with Unnecessary Privileges.

Siemens TeleControl Server Basic | CISA

ICSA-26-015-04: **Siemens SIMATIC and SIPLUS products**

High level vulnerability: Uncontrolled Resource Consumption.

Siemens SIMATIC and SIPLUS products | CISA

ICSA-26-015-05: **Siemens RUGGEDCOM ROS**

Low level vulnerability: Improper Input Validation.

Siemens RUGGEDCOM ROS | CISA

ICSA-26-015-06: **Siemens SINEC Security Monitor**

Medium level vulnerabilities: Improper Authorization, Improper Input Validation.

Siemens SINEC Security Monitor | CISA

ICSA-26-015-07: **Siemens RUGGEDCOM APE1808 Devices**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-26-015-08: **Siemens Industrial Edge Devices**

Critical level vulnerability: Authorization Bypass Through User-Controlled Key.

Siemens Industrial Edge Devices | CISA

ICSA-26-015-09: **Siemens Industrial Edge Device Kit**

Critical level vulnerability: Authorization Bypass Through User-Controlled Key.

Siemens Industrial Edge Device Kit | CISA

ICSA-26-015-10: **Schneider Electric EcoStruxure Power Build Rapsody**

High level vulnerabilities: Double Free, Use After Free.

Schneider Electric EcoStruxure Power Build Rapsody | CISA

ICSA-26-015-11: **Siemens RUGGEDCOM ROX II**

High level vulnerabilities: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Neutralization of Special Elements used in a Command ('Command Injection').

Siemens RUGGEDCOM ROX II | CISA

ICSA-26-015-12: **Siemens SIMATIC CN 4100**

High level vulnerabilities: Improper Neutralization of Special Elements used in a Command ('Command Injection'), Missing Encryption of Sensitive Data, Improper Access Control, Exposure of Sensitive Information to an Unauthorized Actor.

Siemens SIMATIC CN 4100 | CISA

ICSA-22-202-04: **ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update B)**

Critical level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere, Out-of-bounds Read.

ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update B) | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update E)** **Medium** level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write.

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

ICSA-25-352-08: **Axis Communications Camera Station Pro, Camera Station, and Device Manager (Update A)**

Critical level vulnerabilities: Deserialization of Untrusted Data, Improper Certificate Validation, Authentication Bypass Using an Alternate Path or Channel.

Axis Communications Camera Station Pro, Camera Station, and Device Manager (Update A) | CISA

ICSA-26-013-01: **Rockwell Automation 432ES-IG3 Series A**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

Rockwell Automation 432ES-IG3 Series A | CISA

ICSA-26-013-02: **Rockwell Automation FactoryTalk DataMosaix Private Cloud**

High level vulnerability: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Rockwell Automation FactoryTalk DataMosaix Private Cloud | CISA

ICSA-26-013-03: **YoSmart YoLink Smart Hub**

Medium level vulnerabilities: Incorrect Authorization, Generation of Predictable Numbers or Identifiers, Cleartext Transmission of Sensitive Information.

YoSmart YoLink Smart Hub | CISA

ICSA-25-212-01: **Güralp Systems FMUS Series and MIN Series Devices (Update B)**

Critical level vulnerability: Missing Authentication for Critical Function.

Güralp Systems FMUS Series and MIN Series Devices (Update B) | CISA

ICSA-26-008-01: **Hitachi Energy Asset Suite**

Critical level vulnerability: Deserialization of Untrusted Data.

Hitachi Energy Asset Suite | CISA

ICSA-25-140-04: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update C)**

Medium level vulnerability: Execution with Unnecessary Privileges.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update C) | CISA

ICSA-24-184-03: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update B)**

High level vulnerabilities: Allocation of Resources Without Limits or Throttling, Improper Verification of Cryptographic Signature, Uncontrolled Search Path Element, Improper Authentication, Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection').

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update B) | CISA

ICSA-24-338-04: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update A)**

High level vulnerabilities: Uncontrolled Search Path Element, Dead Code.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update A) | CISA

ICSA-22-020-01: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric HMI SCADA (Update A)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incomplete List of Disallowed Inputs, Plaintext Storage of a Password, Buffer Over-read.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric HMI SCADA (Update A) | CISA

ICSA-24-296-01: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update B)**

High level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update B) | CISA

ICSA-26-006-01: **Columbia Weather Systems MicroServer**

High level vulnerabilities: Improper Restriction of Communication Channel to Intended Endpoints, Cleartext Storage in a File or on Disk, Command Shell in Externally Accessible Directory.

Columbia Weather Systems MicroServer | CISA

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

ICS Advisories | CISA

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.

7. ICS alerts

CISA has published alerts in 2026 January:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2009-0556 Microsoft Office PowerPoint Code Injection Vulnerability;
CVE-2025-37164 HPE OneView Code Injection Vulnerability;
CVE-2025-8110 Gogs Path Traversal Vulnerability;
CVE-2026-20805 Microsoft Windows Information Disclosure Vulnerability;
CVE-2026-20045 Cisco Unified Communications Products Code Injection Vulnerability;
CVE-2025-31125 Vite Vitejs Improper Access Control Vulnerability;
CVE-2025-34026 Versa Concerto Improper Authentication Vulnerability;
CVE-2025-54313 Prettier eslint-config-prettier Embedded Malicious Code Vulnerability;
CVE-2025-68645 Synacor Zimbra Collaboration Suite (ZCS) PHP Remote File Inclusion Vulnerability;
CVE-2024-37079 Broadcom VMware vCenter Server Out-of-bounds Write Vulnerability;
CVE-2018-14634 Linux Kernel Integer Overflow Vulnerability;
CVE-2025-52691 SmarterTools SmarterMail Unrestricted Upload of File with Dangerous Type Vulnerability;
CVE-2026-21509 Microsoft Office Security Feature Bypass Vulnerability;
CVE-2026-23760 SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-24061 GNU InetUtils Argument Injection Vulnerability;
CVE-2026-24858 Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-1281 Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability;

Links and more information:
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 One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Secure Connectivity Principles for Operational Technology (OT)

CISA and the UK National Cyber Security Centre (NCSC-UK), in collaboration with federal and international partners, have released Secure Connectivity Principles for Operational Technology (OT) guidance to help asset owners address increasing business and regulatory pressures for connectivity into operational technology (OT) networks.

This guidance outlines eight principles to use as a framework to design, secure, and manage connectivity into OT environments. These principles are particularly critical for operators of essential services.
Links and more information:
Secure Connectivity Principles for Operational Technology (OT) | CISA

Fortinet Releases Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858
Newly disclosed vulnerability Common Vulnerabilities and Exposures (CVE)-2026-24858 [Common Weakness Enumeration (CWE)-288: Authentication Bypass Using an Alternate Path or Channel] allows malicious actors with a FortiCloud account and a registered device to log in to separate devices registered to other users in FortiOS, FortiManager, FortiWeb, FortiProxy, and FortiAnalyzer, if FortiCloud single sign on (SSO) is enabled on devices.
Links and more information:
Fortinet Releases Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858 | CISA

8. ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in January 2026:

- 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

9. 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/