BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 September

2026 September, Critical Systems security feed

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

List of Contents

1. Critical systems security practices, recommendations 2
2. Critical systems security conferences 3
3. Critical systems security incidents 5
4. Book recommendation 9
5. Critical systems security news selection 10
6. Critical systems vulnerabilities 18
7. Critical systems security alerts 28
8. Critical systems security trainings, education 31
9. Critical systems security podcasts 34

1. Critical systems security practices, recommendations

CISA issues Internet Exposure Reduction guidance to reduce risks from IT, OT, ICS and industrial systems

CISA has issued its Internet Exposure Reduction Guidance following a severe cyber campaign in July 2026, where threat actors compromised over 100 exposed systems in the Water and Wastewater Systems (WWS) Sector. Exploiting Programmable Logic Controllers (PLCs) directly connected to cellular modems, attackers altered device configurations, wiped access credentials, and caused operational disruptions. In response, CISA urges critical infrastructure operators to eliminate unnecessary internet-facing pathways, emphasizing that exposed legacy OT devices - often lacking built-in security controls - present a primary target for adversaries.

To mitigate these risks, organizations must systematically map their external attack surface using discovery tools like Shodan, Censys, and Shadowserver, while expanding asset visibility to include vendor, MSSP, and integrator remote access. CISA mandates routing all necessary remote connections through secure, centrally managed gateways or jump hosts rather than exposing PLCs, HMIs, or RTUs directly to the web. Core hygiene measures - including eliminating default passwords, enforcing phishing-resistant MFA, closing unneeded OT ports (such as Modbus or EtherNet/IP), and replacing end-of-support software - remain vital foundational steps.

Industry experts highlight that because OT environments historically prioritize uptime over security, traditional patch management alone is insufficient. Security leaders must adopt Zero Trust principles and granular microsegmentation to limit lateral movement, ensuring that a localized breach on an exposed controller does not turn into a catastrophic operational failure.

Source and more information:

CISA issues Internet Exposure Reduction guidance to reduce risks from IT, OT, ICS and industrial systems - Industrial Cyber

2. Critical systems security conferences

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

SecurityWeek's ICS Cybersecurity Conference 2026

SecurityWeek's ICS Cybersecurity Conference runs 6–8 October 2026 at the W Hotel Nashville — a new host city for what the organiser marks as the event's 25th anniversary.

This is the longest-running event series devoted to industrial cybersecurity: securing the control systems that run power grids, water utilities, pipelines, manufacturing plants and other critical infrastructure. The audience mixes the two communities that OT security requires in the same room — plant and operations engineers on one side, security teams and CISOs on the other.

If you attended in previous years, note the location change: the conference has historically been held in Atlanta, and the 2026 event moves to Nashville.

Nashville, TN, USA; 6th – 8th October 2026

More details can be found on the following website:

SecurityWeek's ICS Cybersecurity Conference 2026 — Oct 6–8, Nashville

Industrial Cybersecurity Day 2026

Industrial Cybersecurity Day 2026 is a free, full-day virtual conference hosted by IIoT World on October 14, 2026. The event features live interactive panels on ransomware defense for manufacturing and energy operations, zero trust architecture for OT networks, IT/OT network segmentation, AI-powered threat detection for industrial control systems, SCADA and PLC vulnerability management, and IEC 62443 compliance. Speakers include CISOs, OT security architects, and incident responders defending production environments across manufacturing, energy, oil and gas, and critical infrastructure. Registration is free for CISOs, CSOs, VPs of cybersecurity, IT/OT security managers, plant managers, and security professionals responsible for operational technology.

Virtual; 14th October 2026

More details can be found on the following website:

Industrial Cybersecurity Day 2026 | IIoT World

13th Cyber and SCADA Security for Power and Utilities Industry 2026

The 13th Cyber & SCADA Security for Power & Utilities Industry 2026 is Europe's leading forum dedicated to safeguarding critical energy infrastructure against rapidly evolving cyber and cyber-physical threats. As digitalisation accelerates across power systems and AI-driven

technologies reshape operations, utilities face increasing risks across SCADA, OT networks, DER platforms, and cross-border grid systems.

Taking place on 15–16 October 2026 in Amsterdam, this conference brings together cybersecurity leaders, CISOs, OT engineers, utilities, TSOs, DSOs, and technology experts to explore next-generation security strategies. Key topics include AI vs AI cyber defence, zero trust OT architecture, real-time anomaly detection, predictive threat intelligence, and securing flexibility markets and virtual power plants.

Attendees will gain practical insights into IT–OT convergence risks, identity-based security, incident response for cyber-physical attacks, and AI-driven resilience frameworks. Through real-world case studies, expert panels, and interactive discussions, the event delivers actionable strategies to protect grid stability, ensure operational continuity, and strengthen Europe's energy cybersecurity posture.

Amsterdam, NH; 15th – 16th October 2026

More details can be found on the following website:

13th Cyber and SCADA Security for Power and Utilities Industry 2026 at Hotel NH Amsterdam Zuid on 15th October, 2026

World OT Summit 2026

The World OT Summit 2026 is a premier international platform dedicated exclusively to OT cyber security, industrial control systems (ICS) security, cyber security for operational technology, and critical infrastructure protection and national security. The summit brings together global policymakers, regulators, CISOs, asset owners, plant operators, and OT cyber security solution providers to address real-world risks facing IT and OT networks, IT and OT systems, and industrial environments.

As global industries accelerate digital transformation, Operational Technology (OT) security has become mission-critical. The convergence of IT and OT systems, OT ICS security, and AI-driven cybersecurity is redefining how critical infrastructure is protected.

This summit goes beyond compliance to focus on practical OT cyber security solutions, artificial intelligence for IT operations (AIOps), and advanced Clarity OT Security frameworks that improve visibility, governance, and resilience across industrial environments.

Abu Dhabi, UAE; 27th – 28th October 2026

More details can be found on the following website:

World OT Summit | 27th - 28th, October 2026 | Cyber Resilient OT

3. Critical systems security incidents

Hackers Disrupt Controls at Minnesota Water Utilities

A coordinated cyberattack disrupted operational technology across more than 30 Minnesota community water systems over a two-day period, forcing utility crews statewide to switch to manual contingency controls. State officials, led by Minnesota IT Services (MNIT) alongside federal agencies including CISA, the EPA, and the FBI, immediately activated incident response protocols. While public health and water quality remained uncompromised - and affected facilities like Braham, South St. Paul, Plymouth, and Maple Plain restored operations rapidly - the incident underscores severe vulnerabilities in internet-exposed municipal infrastructure. Officials have not officially attributed the attack or disclosed the specific mechanisms, but the incident coincided with updated federal advisories warning of ongoing Iranian-affiliated targeting of U.S. industrial control systems.

According to federal warnings, Iranian-linked threat actors (historically associated with IRGC-affiliated groups like CyberAv3ngers) have been actively exploiting internet-connected PLCs, HMIs, and SCADA displays across the water, energy, and government sectors. These adversaries have manipulated or deleted project logic and disabled critical alarm systems, effectively masking unsafe operational states from human operators. To mitigate such risks, federal authorities urge critical infrastructure operators to eliminate direct internet exposure for PLCs and enforce authenticated, restricted remote access. The response in Minnesota was managed under its Whole-of-State Cybersecurity Program, highlighting the necessity of cross-sector threat intelligence sharing during active OT incidents.

The source is available at the following link:

Hackers Disrupt Controls at Minnesota Water Utilities

Colorado Water Utilities Hit by Cyberattacks Targeting OT Systems

In late August, hackers targeted operational technology (OT) systems at two private water utilities in Colorado in an apparent attempt to cause operational disruptions. Although the affected utilities serve fewer than 200 people and few technical details have been disclosed, the attackers managed to target industrial control systems (ICS), alter equipment settings, disable remote access and alarms, and modify pumping cycles. Despite these interventions, the disruptions were brief and caused no impact on water services or public safety.

The Colorado governor's office attributed the incident to "foreign actors" without explicitly naming the affected facilities or confirming the exact perpetrator. State officials noted awareness of an ongoing nation-wide campaign by an Iranian-backed group targeting drinking water and wastewater systems, as warned by the Cybersecurity and Infrastructure Security Agency (CISA), though a direct link to this specific campaign remains unconfirmed. This incident aligns with a broader pattern of cyber threats against the U.S. water sector, which saw attacks on facilities across at least a dozen states in July - including Minnesota, Michigan, Georgia, South Dakota, New Jersey, Wisconsin, and Alabama. In response, CISA urged the

water sector to immediately secure its OT infrastructure, noting that it was aware of 100 internet-exposed water systems targeted in July alone. Additionally, independent security group Infracritical has established a central repository to aggregate technical indicators and operational data from these recent water sector breaches.

The source is available at the following link:

Colorado Water Utilities Hit by Cyberattacks Targeting OT Systems - SecurityWeek

4. Book recommendation

PLC and SCADA Mastery

Unlock the future of industrial possibilities with "PLC and SCADA Mastery." Are you ready to transform your understanding of Industrial Automation and take control of advanced systems like never before? This book offers a practical blueprint to secure operational efficiency and prevent potential disruptions.

Delve deeply into the heart of monitoring systems, SCADA architecture design, and PLC integrations. Discover how to master these technologies to enhance operational visibility and efficiency, helping you eliminate common challenges in industrial settings.

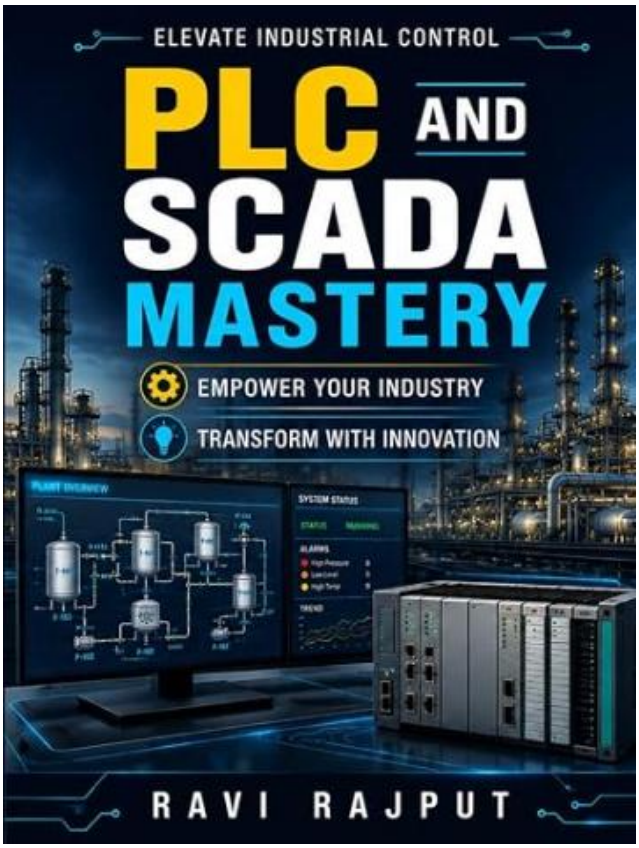
This comprehensive guide is not just about theory; it's about implementation. It offers hands-on techniques and real-world examples that make it possible to visualize and control automated processes efficiently.

Author/Editor: RAVI RAJPUT (Author)

Year of issue: 2026

The book is available at the following link:

Amazon.com: PLC and SCADA Mastery: Network Design in SCADA | SCADA Security Measures | IoT in Industrial SCADA | Operational Visibility Tools | HMI Design Techniques | Advanced Ladder Logic eBook : RAJPUT, RAVI: Kindle Store



5. Critical systems security news selection

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

1. **Coast Guard Establishes Office of Maritime Cybersecurity Policy**
2. **Hackers Exploiting Internet-Exposed OT, Warns UK NCSC**
3. **White House Acts to Shut Out China From US Bulk Power Market**
4. **OpenAI Pledges $1 Billion to Bring Frontier AI to Critical Infrastructure Defenders**
5. **UK Moves to Block High-Risk Tech Suppliers From Critical Infrastructure**
6. **Why Healthcare OT Is a High-Value Cyber Target**
7. **Cyberattacks on food and agriculture can turn disruptions into safety crises, threatening public health and supply chains**
8. **Panzer ransomware targets Italian manufacturer as ESXi capability raises industrial security concerns**
9. **NIST finalizes Meta-Framework to boost manufacturing supply chain visibility, traceability, provenance verification**
10. **White House Touts Local First Approach to Securing Water**
11. **Turn it off and on again, but for critical infrastructure**
12. **Cyberattacks on Two Oil Tankers Prompt Coast Guard, FBI to Board Vessels**
13. **Manufacturing Accounts for 22% of all Ransomware Victims**
14. **Cyber Defense Alone Can't Keep Critical Services Running**
15. **Only 13% of OT Network Segments Are Fully Isolated: Analysis**
16. **Honeywell: OT Security Teams Embrace AI, but Autonomy Still Rare**
17. **Operational Technology Scope Expands as Security Matures**
18. **The Infrastructure Already Has Eyes. We Need to Teach Them What to See.**
19. **Pro-Russia Hacktivists Increase OT Intrusion Claims Across EU**
20. **OT Security Guidance: NIST Drafts Updated Guide, CISA/FBI Advise on ICS Integrators**

Coast Guard Establishes Office of Maritime Cybersecurity Policy

The US Coast Guard has established a dedicated Office of Maritime Cybersecurity Policy as the maritime industry's growing reliance on information and operational technology expands the cyber risks facing ports, vessels, and other critical infrastructure.

The Office of Maritime Cybersecurity Policy (CG-MCP) will serve as the Coast Guard's central authority for developing and implementing policies governing the cyber safety and security of the Marine Transportation System (MTS).

Created under the Director of Inspections and Compliance, the office will also serve as the Coast Guard's primary liaison with industry partners and other government agencies on maritime cybersecurity matters. …

Source and more information:

Coast Guard Establishes Office of Maritime Cybersecurity Policy - SecurityWeek

Hackers Exploiting Internet-Exposed OT, Warns UK NCSC

Britain's National Cyber Security Center warned that attacks on operational technology systems have been increasing across multiple sectors globally, making securing internet-facing devices an imperative.

Although disruptions have been limited, the British cybersecurity agency learned that OT attacks will continue to develop as new technology enhances state and non-state actors' capabilities and geopolitical instability spurs offensive cyber operations.

"Targeting of operational technology reinforces the need for organizations to understand what is exposed to the internet, address avoidable vulnerabilities and build long-term cyber resilience," the advisory said Thursday. …

Source and more information:

Hackers Exploiting Internet-Exposed OT, Warns UK NCSC

White House Acts to Shut Out China From US Bulk Power Market

A broad Trump administration plan to shut adversary nations, including China, out of the equipment supply chain for the U.S. bulk electric power market has left the industry in regulatory uncertainty, just as demand for electricity is spiking nationwide due the ballooning power demands of data centers and severe weather caused by climate change.

A sweeping executive order President Donald Trump signed last week, little noticed outside the electricity sector, declared a national emergency in the bulk power supply industry owing to cybersecurity vulnerabilities and potential backdoors in foreign-manufactured equipment.

Industry knew this reckoning was coming since the first Trump administration, said Patrick Miller, CEO of Ampyx Cyber, an OT security services company. …

Source and more information:

White House Acts to Shut Out China From US Bulk Power Market

OpenAI Pledges $1 Billion to Bring Frontier AI to Critical Infrastructure Defenders

Daybreak is OpenAI's continuously running agentic loop that brings the power of frontier AI to simplify complex security investigations, validation, remediation and reporting. The earlier Daybreak Blue supports common defensive work with OpenAI mainline models; while Daybreak Red gives approved organizations access to specialized cyber models for more sensitive and technically demanding work.

The new Daybreak for Frontline Defenders was announced on September 3, 2026, as a $1 billion subsidy for Frontline Defenders to access Daybreak. These frontline defenders are defenders required to protect the critical industry, often under-funded and usually with aging equipment. While the commitment is global, the announcement makes it clear that initial priority will be given to American companies. …

Source and more information:

OpenAI Pledges $1 Billion to Bring Frontier AI to Critical Infrastructure Defenders - SecurityWeek

UK Moves to Block High-Risk Tech Suppliers From Critical Infrastructure

The UK Cyber Security and Resilience Bill (CSRB) has been given late amendments specifically targeting the supply chain threat against the nation's critical infrastructure.

The UK CSRB – not to be confused with the US Cyber Safety Review Board (CSRB) – was introduced to Parliament in November 2025. It has successfully completed all necessary steps through the House of Commons, has moved to the House of Lords (as HL Bill 32) and is now close to receiving Royal Assent. Royal Assent is the point at which the Bill becomes an Act of Parliament and part of UK legislation, where it transitions into the Cyber Security and Resilience (Network and Information Systems) Act. …

Source and more information:

UK Moves to Block High-Risk Tech Suppliers From Critical Infrastructure - SecurityWeek

Why Healthcare OT Is a High-Value Cyber Target

Recent Iranian-affiliated cyber activity against U.S. water utilities could signal a broader threat to healthcare operational technology, where exposed devices and tight security resources increase risk, said James Turgal, vice president of global risk and board relations at Optiv.

Rural hospitals, independent clinics and regional health centers face particular pressure because they often operate on narrow margins while relying on internet-connected

equipment, including pumps, valves, oxygen systems, dialysis machines and ventilators, said Turgal, who served 22 years at the FBI. …

Source and more information:

Why Healthcare OT Is a High-Value Cyber Target

Cyberattacks on food and agriculture can turn disruptions into safety crises, threatening public health and supply chains

Food and agriculture tends to be an overlooked corner of the cybersecurity conversation despite being critical infrastructure where a cyber incident isn't just a business problem, but can quickly escalate into a food-safety and public-health crisis. The sector operates on unforgiving timelines. Products spoil. Supply chains depend on perfect handoffs. Margins are already razor-thin. A week of downtime doesn't just mean lost revenue – it means products rotting in storage, broken promises to grocery chains that were counting on that supply, empty shelves. …

Source and more information:

Cyberattacks on food and agriculture can turn disruptions into safety crises, threatening public health and supply chains - Industrial Cyber

Panzer ransomware targets Italian manufacturer as ESXi capability raises industrial security concerns

New research from cybersecurity researcher Andrea Fortuna detailed that Panzer ransomware emerged in August as a ransomware-as-a-service operation and, within its first month, claimed victims across 11 countries, including two Italian organizations. The Italian victims were Doimo Cucine, a kitchen manufacturer based near Treviso, listed on Aug. 17, and NTE Italia, a telecommunications engineering and consulting firm based in Catanzaro, listed four days later. However, the claims have not been publicly confirmed by either organization. …

Source and more information:

Panzer ransomware targets Italian manufacturer as ESXi capability raises industrial security concerns - Industrial Cyber

NIST finalizes Meta-Framework to boost manufacturing supply chain visibility, traceability, provenance verification

The U.S. National Institute of Standards and Technology's National Cybersecurity Center of Excellence (NCCoE) published on Wednesday final version of NIST Internal Report (IR) 8536, Supply Chain Traceability Principles: A Manufacturing Meta-Framework. Building on NIST IR 8419, the publication establishes foundational principles for manufacturing supply chain traceability through a technology-neutral Meta-Framework designed to organize, link, and

query traceability data across diverse systems and stakeholders. These concepts directly support a forthcoming Minimum Viable Product (MVP) Reference Implementation (RI), which uses real-world use cases to examine practical mechanics of cross-industry data sharing in a controlled lab environment, focusing on interoperability, cybersecurity, governance, and traceability data analysis. …

Source and more information:

NIST finalizes Meta-Framework to boost manufacturing supply chain visibility, traceability, provenance verification - Industrial Cyber

White House Touts Local First Approach to Securing Water

A White House effort dubbed Project Watershed 250 that's meant to help small or rural water utilities in Texas secure their systems against hackers with free technology donated by cybersecurity vendors will expand nationwide, the country's top cyber official said Thursday.

Water utility cybersecurity has been under-resourced for years, White House National Cyber Director Sean Cairncross told the Billington Cybersecurity Summit, for reasons "having to do with capacity, some of it resourcing, some of it just the diffusion of its management." …

Source and more information:

White House Touts Local First Approach to Securing Water

Turn it off and on again, but for critical infrastructure

Researchers at KTH Royal Institute of Technology built a container replica of a segmented industrial network, attacked it repeatedly across 14 days of running time, and used the captured traffic to train a defense agent that decides on its own when to intervene.

The agent sees six numbers per interval: packet counts crossing the network’s segments and moving to and from individual machines. From those counts it infers how far an intruder has progressed, and acts.

It can do nothing, reset one of three supervisory hosts, reset one of two water tank processes, or reset every host in the supervisory and control subnets at once. …

Source and more information:

Turn it off and on again, but for critical infrastructure - Help Net Security

Cyberattacks on Two Oil Tankers Prompt Coast Guard, FBI to Board Vessels

Two oil tankers bound for Texas were boarded by US Coast Guard and FBI personnel last month after cyberattacks disrupted the vessels during their voyage toward the United States, according to a CBS News report citing US officials.

One of the ships, the VL Prosperity, is a Liberian-flagged crude tanker that left Egypt on August 1 en route to Galveston, Texas, per vessel-tracking records cited by CBS News.

Iran's Mehr News Agency reported on August 20 that the cyberattack had allegedly occurred on August 7 as the tanker passed through the Strait of Gibraltar. Citing a crew member, the Iranian outlet said the intrusion reached the engine room, with hackers slowing coolant flow, raising engine speed and interfering with fuel delivery. …

Source and more information:

Cyberattacks on Two Oil Tankers Prompt Coast Guard, FBI to Board Vessels - SecurityWeek

Manufacturing Accounts for 22% of all Ransomware Victims

Manufacturing is viewed as a high-value target for ransomware actors for a number of reasons. One factor is that a successful attack can result in significant downtime for victim organizations, which in turn leads to substantial financial losses, potentially making them more likely to agree to pay an extortion demand to resume operations.

The financial impact of such incidents was highlighted in the attack on UK car manufacturing giant Jaguar Land Rover (JLR) in 2025, which is estimated to have cost the UK economy £1.9bn ($2.5bn).

Another factor is growing IT-OT convergence in the sector, making it easier for threat actors to compromise industrial systems. …

Source and more information:

Manufacturing Accounts for 22% of all Ransomware Victims - Infosecurity Magazine

Cyber Defense Alone Can't Keep Critical Services Running

State CIOs are responsible for the technology platforms, networks and digital services that keep state government running. Now they are being asked to apply that expertise across a far larger and more fragmented landscape of locally operated water systems, hospitals and other critical infrastructure, where a cyberattack can disrupt physical services and threaten public safety.

That concern is nearly universal. In the 2026 NASCIO State CIO Survey, 88% of state CIOs identified cyberattacks against critical infrastructure as a high concern. A new report from the association recommends that states inventory essential systems and concentrate resources where they will have the greatest impact. …

Source and more information:

Cyber Defense Alone Can't Keep Critical Services Running

Only 13% of OT Network Segments Are Fully Isolated: Analysis

Most organizations running operational technology (OT) or connected medical devices do not keep those systems on their own dedicated network segments, according to new research from Forescout's Vedere Labs.

The cybersecurity firm's researchers examined 47,700 network segments holding more than 2.5 million devices across 209 organizations, sorting each device into one of four categories: IT, OT, IoT, or medical (IoMT).

At the surface level, segmentation looks reasonably solid. The researchers found that 62% of segments contained devices from a single category, and the most common setups were IT devices alone (54%) or paired with IoT gear (26%). …

Source and more information:

Only 13% of OT Network Segments Are Fully Isolated: Analysis - SecurityWeek

Honeywell: OT Security Teams Embrace AI, but Autonomy Still Rare

Honeywell released its 2026 OT Cybersecurity Benchmark Report on Tuesday, and the findings point to a disconnect between how industrial organizations rate their operational technology (OT) security programs and how prepared they actually are. The report also examines AI's impact on OT security.

Among 603 surveyed leaders across critical infrastructure sectors, 88% characterized their OT security programs as mature or design-led, yet only 21% maintain a complete inventory of their OT assets.

Respondents worked across critical infrastructure sectors, including energy, oil and gas, healthcare, maritime, and manufacturing, with participation spanning the Americas, EMEA and APAC regions. …

Source and more information:

Honeywell: OT Security Teams Embrace AI, but Autonomy Still Rare - SecurityWeek

Operational Technology Scope Expands as Security Matures

Serious cybersecurity incidents involving operational technology systems carry a cost, averaging over 16 hours of downtime and losses of up to $500,000 per hour. As a result, more industrial organizations report putting plans and capabilities in place designed specifically to prevent such downtime, or to minimize operational disruption when it does occur.

Those findings come from Honeywell Technologies' inaugural 2026 Operational Technology Cybersecurity Benchmark Report, based on studies conducted by ISMG advisory firm CyberTheory. …

Source and more information:

Operational Technology Scope Expands as Security Matures

The Infrastructure Already Has Eyes. We Need to Teach Them What to See.

Industrial cybersecurity has spent years getting better at seeing what is happening inside networks. We have more asset discovery, monitoring, segmentation, vulnerability management and detection capability than ever before.

That visibility matters.

But once a cyber incident begins affecting an operational environment, another question becomes more important:

What happens to the physical process when we can no longer trust the digital systems controlling it? …

Source and more information:

The Infrastructure Already Has Eyes. We Need to Teach Them What to See. - Industrial Cyber

Pro-Russia Hacktivists Increase OT Intrusion Claims Across EU

Claims of cyberattacks against operational technology and industrial environments increased significantly in 2025 - particularly those involving pro-Russia hacktivist groups, the European Union Agency for Cybersecurity warned.

ENISA released its annual Threat Landscape report last week, finding that ideology-driven malicious cyberattacks accounted for 57.3% of all incidents the agency recorded in 2025, followed by financially motivated activity at about 30%. In total, there were 4,709 hacktivist claims against European Union member states last year, 89.5% of which involved distributed denial-of-service attacks. The rest involved unauthorized access. …

Source and more information:

Pro-Russia Hacktivists Increase OT Intrusion Claims Across EU

OT Security Guidance: NIST Drafts Updated Guide, CISA/FBI Advise on ICS Integrators

NIST has published a draft update to its operational technology security guide, and CISA and the FBI have issued a fact sheet on the risks of working with third-party ICS integrators.

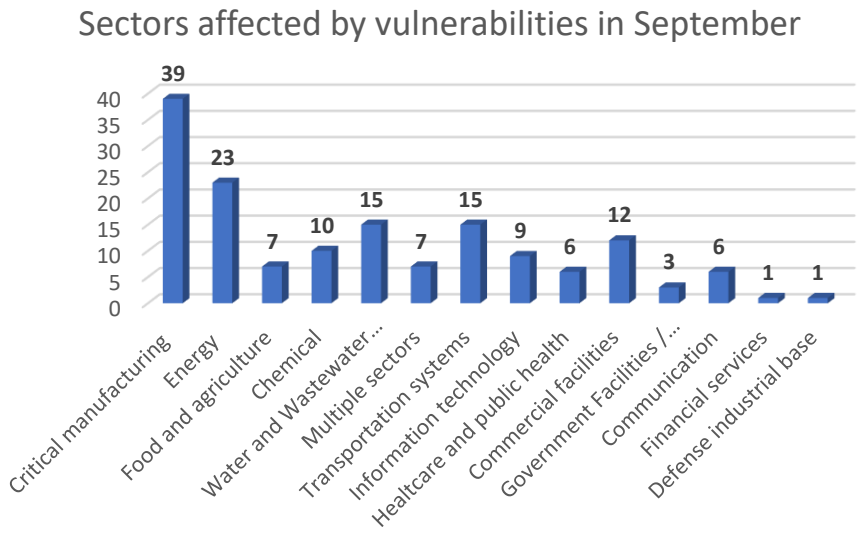
NIST this week released a draft of Special Publication 800-82 Revision 4, titled Guide to Operational Technology (OT) Security. Public comments are due by November 30, 2026. The document covers how to secure OT while accounting for the performance, reliability and safety demands specific to these systems. …

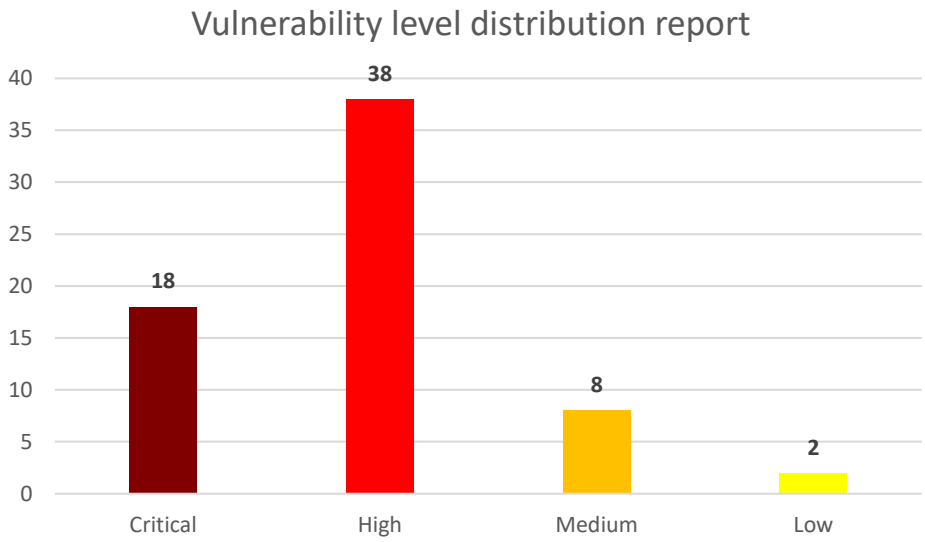
Source and more information:

OT Security Guidance: NIST Drafts Updated Guide, CISA/FBI Advise on ICS Integrators - SecurityWeek

6. Critical systems vulnerabilities

In September 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-26-272-01: **Lantronix G520 Series Cellular Gateway**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Verification of Cryptographic Signature.

Lantronix G520 Series Cellular Gateway | CISA

ICSA-26-272-02: **Toptech TMS7 and TopHAT**

Critical level vulnerabilities: Files or Directories Accessible to External Parties, Unrestricted Upload of File with Dangerous Type, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Session Fixation, Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Toptech TMS7 and TopHAT | CISA

ICSA-26-272-03: **VIVOTEK Camera Firmware**

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

VIVOTEK Camera Firmware | CISA

ICSA-26-272-04: **Baicells Nova 430H**

High level vulnerability: Uncaught Exception.

Baicells Nova 430H | CISA

ICSA-26-272-05: **Anjvision YSSD-RTMP-H5**

Critical level vulnerabilities: Initialization of a Resource with an Insecure Default, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Verification of Cryptographic Signature, Use of Hard-coded Credentials, Active Debug Code, Improper Check for Unusual or Exceptional Conditions, Server-Side Request Forgery (SSRF), Insufficiently Protected Credentials, Use of Weak Credentials.

Anjvision YSSD-RTMP-H5 | CISA

ICSA-26-272-06: **MikroTik RouterOS**

Critical level vulnerability: Integer Underflow (Wrap or Wraparound).

MikroTik RouterOS | CISA

ICSA-26-272-07: **Viidure Dashcam Android Application**

Critical level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Use of Hard-coded Credentials.

Viidure Dashcam Android Application | CISA

ICSA-26-267-01: **Botslab G980H Dashcams**

High level vulnerabilities: Incorrect Authorization, Insufficient Session Expiration, Generation of Predictable Numbers or Identifiers, Authentication Bypass by Capture-replay,

Use of Weak Credentials, Missing Authentication for Critical Function, Insertion of Sensitive Information into Log File, Use of Hard-coded Cryptographic Key, Insufficient Verification of Data Authenticity, Out-of-bounds Write, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Use of Hard-coded Credentials, Cleartext Transmission of Sensitive Information.

Botslab G980H Dashcams | CISA

ICSA-26-267-02: **Eufy Omni C20, Omni X10 Pro**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Use of Hard-coded Credentials, Improper Certificate Validation.

Eufy Omni C20, Omni X10 Pro | CISA

ICSA-26-258-02: **Wärtsilä FOS-Onboard (Update A)**

High level vulnerability: Use of Hard-coded Cryptographic Key.

Wärtsilä FOS-Onboard (Update A) | CISA

ICSA-26-209-02: **Siemens Mendix Runtime (Update A)**

Critical level vulnerability: Insecure Inherited Permissions.

Siemens Mendix Runtime (Update A) | CISA

ICSA-26-265-01: **lwIP TCP/IP Stack MQTT Client Application**

Critical level vulnerability: Out-of-bounds Write.

lwIP TCP/IP Stack MQTT Client Application | CISA

ICSA-26-265-02: **lwIP (Lightweight IP)**

High level vulnerability: Double Free.

lwIP (Lightweight IP) | CISA

ICSA-26-265-03: **Siemens Siveillance Control**

Critical level vulnerability: Unrestricted Upload of File with Dangerous Type.

Siemens Siveillance Control | CISA

ICSA-26-265-04: **Siemens SIPLUS and SIMATIC Products**

High level vulnerability: Incorrect Resource Transfer Between Spheres.

Siemens SIPLUS and SIMATIC Products | CISA

ICSA-26-265-05: **Siemens Desigo CC family**

High level vulnerability: Improper Control of Generation of Code ('Code Injection').

Siemens Desigo CC family | CISA

ICSA-26-265-06: **Siemens Industrial Edge Management**

Critical level vulnerability: Weak Password Recovery Mechanism for Forgotten Password.

Siemens Industrial Edge Management | CISA

ICSA-26-265-07: **Siemens SIMOVE Fleetmanager and SIPLANT**

High level vulnerability: Relative Path Traversal.

Siemens SIMOVE Fleetmanager and SIPLANT | CISA

ICSA-26-265-08: **Siemens WTV676 and WTV776**

Medium level vulnerability: Improper Validation of Specified Type of Input.

Siemens WTV676 and WTV776 | CISA

ICSA-26-265-09: **OpenPLC Runtime v3**

Medium level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

OpenPLC Runtime v3 | CISA

ICSA-26-260-01: **Bransys ELD**

High level vulnerabilities: Use of Hard-coded Credentials, Cleartext Transmission of Sensitive Information.

Bransys ELD | CISA

ICSA-26-260-02: **Mitsubishi Electric GX Works3**

High level vulnerability: Incorrect Implementation of Authentication Algorithm.

Mitsubishi Electric GX Works3 and Motion Control Settings | CISA

ICSA-26-260-03: **Hitachi Energy FACTS Control Platform (FCP)**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Data Query Logic, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Authentication Bypass by Capture-replay, Missing Authentication for Critical Function, URL Redirection to Untrusted Site ('Open Redirect').

Hitachi Energy FACTS Control Platform (FCP) | CISA

ICSA-26-260-04: **Schneider Electric Modicon M340 Controller and Communication Modules**

High level vulnerability: Improper Input Validation.

Schneider Electric Modicon M340 Controller and Communication Modules | CISA

ICSA-26-260-05: **Schneider Electric NetBotz 5 750/755**

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

Schneider Electric NetBotz 5 750/755 | CISA

ICSA-26-260-06: **ABB Ability Edgenius**

High level vulnerability: Incorrect Resource Transfer Between Spheres.

ABB Ability Edgenius | CISA

ICSA-26-260-07: **Schneider Electric PowerChute Serial Shutdown**

Medium level vulnerability: Improper Restriction of Excessive Authentication Attempts.

Schneider Electric PowerChute Serial Shutdown | CISA

ICSA-26-211-07: **Mitsubishi Electric CC-Link IE TSN Communication Protocol (Update A)**

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

Mitsubishi Electric CC-Link IE TSN Communication Protocol (Update A) | CISA

ICSA-26-258-01: **Digital Watchdog VMAX, DVR and NVR Product Lineups**

Critical level vulnerabilities: Missing Authentication for Critical Function, Use of Hard-coded Credentials, Missing Authorization, Predictable Seed in Pseudo-Random Number Generator (PRNG).

Digital Watchdog VMAX DVR and NVR Product Lineups | CISA

ICSA-26-258-02: **Wärtsilä FOS-Onboard**

Critical level vulnerability: Use of Hard-coded Cryptographic Key.

Wärtsilä FOS-Onboard | CISA

ICSA-26-258-03: **mySCADA myPRO Manager**

Critical level vulnerabilities: Missing Authorization, Missing Authentication for Critical Function.

mySCADA myPRO Manager | CISA

ICSA-26-258-04: **Schneider Electric SCADAPack x70 Products**

Medium level vulnerability: Insufficiently Protected Credentials.

Schneider Electric SCADAPack x70 Products | CISA

ICSA-26-258-05: **Siemens Reyrolle 7SR5**

Critical level vulnerabilities: Integer Overflow or Wraparound, Improper Neutralization of Delimiters, Use of Out-of-range Pointer Offset, Missing Authentication for Critical Function, Insufficient Entropy, Improper Input Validation, Out-of-bounds Write, Allocation of Resources Without Limits or Throttling, Authentication Bypass Using an Alternate Path or Channel, Insertion of Sensitive Information Into Debugging Code, Download of Code Without Integrity Check.

Siemens Reyrolle 7SR5 | CISA

ICSA-26-258-06: **Siemens Mendix SAML**

High level vulnerability: Improper Verification of Cryptographic Signature.

Siemens Mendix SAML | CISA

ICSA-26-258-07: **Siemens Teamcenter**

Medium level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Siemens Teamcenter | CISA

ICSA-26-258-08: **CareCam CM2507**

High level vulnerabilities: Missing Authentication for Critical Function, Empty Password in Configuration File, Inclusion of Functionality from Untrusted Control Sphere, Use of Password Hash With Insufficient Computational Effort, Cleartext Storage of Sensitive Information.

CareCam CM2507 | CISA

ICSMA-26-253-01: **NextGen Mirth Connect**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Restriction of XML External Entity Reference.

NextGen Healthcare Mirth Connect | CISA

ICSMA-26-253-02: **Orthanc DICOM Server**

High level vulnerability: Integer Overflow or Wraparound.

Orthanc DICOM Server | CISA

ICSA-26-253-01: **AVEVA Pipeline Integrity Monitor**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Use of a Broken or Risky Cryptographic Algorithm, Missing Authorization, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

AVEVA Pipeline Integrity Monitor | CISA

ICSA-26-183-01: **ST Engineering iDirect iQ-Series Terminals (Update A)**

High level vulnerabilities: Missing Authentication for Critical Function, Cross-Site Request Forgery (CSRF), Missing Authorization, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

ST Engineering iDirect iQ-Series Terminals (Update A) | CISA

SSA-434797: **Buffer Overflow Vulnerability in OpenSSL affecting Siemens Products (Update 1.3.)**

High level vulnerability: Out-of-bounds Write.

SSA-434797

SSA-331739: **Privilege Escalation Vulnerability in WIBU CodeMeter Runtime Affecting Siemens Products (Update 1.2.)**

High level vulnerability: Least Privilege Violation.

SSA-331739

SSA-327438: **Multiple Vulnerabilities in SCALANCE LPE9403 (Update 1.2.)**

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.

SSA-327438

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update 1.9.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-229470: **Multiple Vulnerabilities in SICAM 8 Products Before V26.20 (Update 1.1.)**

High level vulnerabilities: Active Debug Code, Initialization of a Resource with an Insecure Default, Unverified Password Change.

SSA-229470

SSA-216014: **Vulnerabilities in EFI variable of SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs (Update 1.6.)**

High level vulnerability: Protection Mechanism Failure.

SSA-216014

SSA-019113: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1.6 (Update 1.1.)**

High level vulnerabilities: Multiple.

SSA-019113

ICSA-26-251-01: **CareCam Pro IP Cameras**

Medium level vulnerability: Use of Hard-coded Credentials.

CareCam Pro IP Cameras | CISA

ICSA-26-169-07: **Schneider Electric Easergy, EcoStruxture, PowerLogic, and Saitel Products (Update A)**

High level vulnerability: Insufficient Entropy.

Schneider Electric Easergy, EcoStruxture, PowerLogic, and Saitel Products (Update A) | CISA

ICSA-26-202-01: **Tycon Systems TPDIN-Monitor-WEB2 (Update A)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Cleartext Storage of Sensitive Information.

Tycon Systems TPDIN-Monitor-WEB2 (Update A) | CISA

ICSA-26-246-01: **OPCFoundation OPC UA LocalDiscoveryServer (LDS)**

Low level vulnerability: Execution with Unnecessary Privileges.

OPCFoundation OPC UA LocalDiscoveryServer (LDS) | CISA

ICSA-26-246-02: **IXON VPN Client**

Critical level vulnerability: Improper Neutralization of CRLF Sequences ('CRLF Injection').

IXON VPN Client | CISA

ICSA-26-246-03: **Rockwell Automation ControlFLASH**

High level vulnerability: Missing Authentication for Critical Function.

Rockwell Automation ControlFLASH | CISA

ICSA-26-246-04: **Rockwell Automation ArmorStart LT**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Allocation of Resources Without Limits or Throttling.

Rockwell Automation ArmorStart LT | CISA

ICSA-26-246-05: **Rockwell Automation 1756-ENBT Module**

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

Rockwell Automation 1756-ENBT Module | CISA

ICSA-26-246-06: **Inductive Automation Ignition**

High level vulnerability: Incorrect Default Permissions.

Inductive Automation Ignition | CISA

ICSA-26-246-07: **Pyramid Solutions NetStaX EtherNet/IP Stack**

Critical level vulnerability: Stack-based Buffer Overflow.

Pyramid Solutions NetStaX EtherNet/IP Stack | CISA

ICSA-26-246-08: **Tycon Systems TPDIN-Monitor-WEB3**

High level vulnerabilities: Use of Hard-coded Credentials, Cross-Site Request Forgery (CSRF), Missing Authorization.

Tycon Systems TPDIN-Monitor-WEB3 | CISA

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

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

ICSA-26-202-09: **Rockwell Automation 1734 POINT I/O (Update A)**

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

Rockwell Automation 1734 POINT I/O (Update A) | CISA

ICSA-26-244-01: **Rockwell Automation RSLinx Classic**

High level vulnerabilities: Integer Overflow or Wraparound, Integer Underflow (Wrap or Wraparound), Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

Rockwell Automation RSLinx Classic | CISA

ICSA-26-244-02: **Rockwell Automation Redundancy Module Configuration Tool**

High level vulnerability: Incorrect Default Permissions.

Rockwell Automation Redundancy Module Configuration Tool | CISA

ICSA-26-244-03: **Rockwell Automation Logix Platform**

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

Rockwell Automation Logix Platform | CISA

ICSA-26-244-04: **Rockwell Automation FactoryTalk Activation Manager**

High level vulnerability: Improper Restriction of Excessive Authentication Attempts.

Rockwell Automation FactoryTalk Activation Manager | CISA

ICSA-26-244-05: **Rockwell Automation ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

Rockwell Automation ControlLogix, CompactLogix, CompactLogix 5480, GuardLogix, Compact GuardLogix | CISA

ICSA-26-244-06: **Rockwell Automation Historian ME**

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

Rockwell Automation Historian ME | 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. Critical systems security alerts

CISA has published alerts in 2026 September:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-9586 Sangoma Switchvox SQL Injection Vulnerability;
CVE-2026-48710 Kludex Starlette HTTP Request/Response Smuggling Vulnerability;
CVE-2026-49869 Kestra OSS OS Command Injection Vulnerability;
CVE-2026-59822 BerriAI LiteLLM Improper Authentication Vulnerability;
CVE-2026-82329 JFrog Artifactory Improper Authentication Vulnerability;
CVE-2026-83548 SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability;
CVE-2026-83549 SonicWall SMA1000 Appliances OS Command Injection Vulnerability;
CVE-2026-85046 Google Chromium V8 Type Confusion Vulnerability;
CVE-2026-75650 Adobe Commerce and Magento Improper Neutralization of Special Elements Used in a Template Engine Vulnerability;
CVE-2026-81963 Microsoft Windows Link Following Vulnerability;
CVE-2026-85880 Microsoft Windows Heap-Based Buffer Overflow Vulnerability;
CVE-2026-86218 N-able N-central Static Code Injection Vulnerability;
CVE-2025-25249 Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability;
CVE-2026-19490 Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-87491 Google Chromium V8 Out of Bounds Write Vulnerability;
CVE-2026-20079 Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability;
CVE-2026-67277 MikroTik RouterOS Missing Authentication for Critical Function Vulnerability;
CVE-2026-86060 MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability;
CVE-2026-42016 JFrog Artifactory Incorrect Authorization Vulnerability;
CVE-2026-42018 JFrog Artifactory Improper Authentication Vulnerability;
CVE-2026-84869 ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability;
CVE-2026-85706 GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability;
CVE-2026-76461 Cisco Secure Email Gateway SQL Injection Vulnerability;
CVE-2026-58704 Google Pixel Improper Authorization Vulnerability;
CVE-2026-76460 Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability;
CVE-2026-87886 Acronis Backup Incorrect Default Permissions Vulnerability;
CVE-2025-39964 Linux Kernel Race Condition Vulnerability;
CVE-2026-53266 Linux Kernel Out-of-Bounds Write Vulnerability;

CVE-2025-39682 Linux Kernel Improper Check for Unusual or Exceptional Conditions Vulnerability;
CVE-2026-7273 Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability;
CVE-2026-85102 Check Point Multiple Products Improper Certificate Validation Vulnerability;
CVE-2026-93616 Check Point Multiple Products Path Traversal Vulnerability;
CVE-2026-93952 Arista VeloCloud Orchestrator Improper Input Validation Vulnerability;
CVE-2026-94127 F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability;
CVE-2026-5430 WSO2 Multiple Products Path Traversal Vulnerability;
CVE-2026-71362 Adobe Commerce and Magento Incorrect Authorization Vulnerability;
CVE-2026-65660 Microsoft SharePoint Code Injection Vulnerability;
CVE-2026-67279 Mikrotik RouterOS Improper Enforcement of Behavioral Workflow Vulnerability;
CVE-2026-87902 WordPress Core Remote File Inclusion Vulnerability;
CVE-2026-88771 Citrix NetScaler Improper Input Validation Vulnerability;
CVE-2026-88772 Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability;
CVE-2026-86950 Apple Multiple Products Out-of-Bounds Write Vulnerability;
Links and more information:
CISA Adds Seven Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three 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 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 Four Known Exploited Vulnerabilities to Catalog | CISA
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 Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway
CISA is amplifying Citrix's disclosure of eight new vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway products: CVE-2026-88771, CVE-2026-

88772, CVE-2026-88773, CVE-2026-88774, CVE-2026-88775, CVE-2026-88776, CVE-2026-88777, and CVE-2026-88778.
CISA has added CVE-2026-88771 and CVE-2026-88772 to its Known Exploited Vulnerabilities (KEV) Catalog. Both are critical, zero-day vulnerabilities that can independently enable remote code execution. CISA has received reports and partner. threat intelligence confirming that threat actors are actively exploiting these vulnerabilities globally.
Links and more information:
Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway | CISA

8. Critical systems security trainings, education

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

- Internet of Things (IoT) Practitioner (Exam ITP-110)
- Internet of Things (IoT) Security (Exam ITS-110)

Coursera | Online Courses From Top Universities. Join for Free

- 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)

ICS Training Available Through CISA | CISA

- 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

ICS410: ICS/SCADA Security Essentials | SANS Institute

- 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

ICS/SCADA Cyber Security

- SCADA security training

SCADA Security Training | SCADA Security Training Course

- 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

ICSP Training Boot Camp (OT/ICS Certified Security Professional) | Infosec

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

Industrial Control System and SCADA Cybersecurity Training - Tonex Training

- Bsigroup: Certified Lead SCADA Security Professional training course

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

- The Industrial Cyber Security Certification Course

Certified Industrial Cybersecurity Professional Certification | CICP Course

- Secure IACS by ISA-IEC 62443 Standard

Secure IACS by ISA-IEC 62443 Standard

- Dragos Academy ICS/OT Cybersecurity Training

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

- ISA/IEC 62443 Training for Product and System Manufacturers

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

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

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

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

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

- Lead SCADA Security Manager

Lead SCADA Security Manager | PECB

- OT/IT Security Training

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

- OT Railway Cybersecurity (OTCS)

OT Railway Cybersecurity (OTCS) Training - Informa Academy

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

OT Security Expert - OPSWAT Academy

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

CTR-008 - OT-Security Awareness E-Learning Course | Yokogawa Europe

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

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

- Cybersecurity for Industrial Automation (ICS/SCADA) and OT

https://www.imfacademy.com/security-management/ot-cybersecurity.php

- Operational Technology (OT) Security Learning Path

Infosec's Operational Technology (OT) Security Learning Path

9. Critical systems security 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/