BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 May

2026 May, 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

Gen AI: A game-changer for OT security Opportunities, Challenges, and the Road to Resilience

Just as Gen AI is reshaping the world of sports – influencing everything from personalized training and nutrition plans for athletes to enhancing the fan experience –it is having a profound effect on industrial environments. As traditional operational technology (OT) merges with cutting-edge IT systems, the complexity of securing these hybrid landscapes increases exponentially. Now, with the rise of generative AI (Gen AI), the cybersecurity game is evolving at a rapid - and sometimes unsettling - pace.

The promise of digital transformation - integrating Industrial Internet of Things (IIoT) devices, cloud platforms, and AI-powered analytics - offers undeniable benefits. Operations become more efficient, productive, and sustainable. However, every new digital connection introduces a new potential point of vulnerability. It's no longer enough to focus security efforts solely on traditional IT networks; organizations must embed security deeply within their digital strategies.

To achieve this, organizations should implement strong encryption, strict access controls, and carry out ongoing security evaluations. As OT systems evolve to include virtualization technologies like Programmable Logic Controllers (PLCs) at the edge and localized data centers, it's clear that transformation isn't just about embracing the cloud. Local compute solutions now play a vital role in aligning security with the unique demands of industrial environments.

We strongly recommend looking into the following (more at the link):

- Raising the bar
- Gen AI in a head-to-head battle – with itself
- Offense is often the best defense
- Getting the best players onto your team
- The endgame

Source and more information:

https://www.orange-business.com/en/blogs/gen-ai-game-changer-ot-security-opportunities-challenges-road-resilience

2. Critical systems security conferences

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

ID User Conference 2026

Industrial Defender is excited to host our next in-person User Summit in Minneapolis, Minnesota, with sessions taking place at Xcel Energy headquarters.

Join us June 1–3 for a customer-only event where you'll gain firsthand insight into the latest product innovations, participate in interactive discussions, explore what's ahead on the roadmap, and connect with fellow Industrial Defender users and industry peers.

Minneapolis, Minnesota, USA; 1st – 3rd June 2026

More details can be found on the following website:

https://www.industrialdefender.com/save-the-date-2026

2026 OT Cybersecurity Summit

As industrial and government organizations continue to modernize operations, the ability to secure OT and critical infrastructure without increasing complexity will be essential. Get clear, actionable guidance on reducing risk, improving resilience and keeping operations safe at the OT Security Summit. Gather insights from industry analysts, OT security experts, and practitioners on reducing risk across converged IT/OT environments, improving visibility and segmentation, and accelerating your CPS cybersecurity journey to resilient operations.

Virtual summit:

- AMER: June 9 2026 | 9:00 AM PDT
- India and SAARC: June 10 2026 | 10:30 AM IST
- APAC: June 10 2026 | 11:30 AM SGT
- EMEA: June 11 2026 | 11:00 AM CEST

More details can be found on the following website:

https://www.fortinet.com/corporate/about-us/events/events/ot-summit

ISA OT Cybersecurity Summit

ISA developed ISA/IEC 62443, the world's only consensus-based automation and control systems cybersecurity standards. In addition to developing and maintaining these standards, ISA offers training and credentialing on cybersecurity; certifies products, processes and systems through its ISA Secure certification; and raises awareness about the importance of OT cybersecurity through its membership consortium, the ISA Global Cybersecurity Alliance (ISAGCA).

Who Should Attend: Individuals who are directly involved in securing operational technology (OT) systems within their organizations at the management level or higher…

Prague, Czech Republic; 16th -18th June 2026

More details can be found on the following website:

https://otcs.isa.org/

ICS / SCADA Cybersecurity Symposium

Organizations in manufacturing, transportation, energy, water treatment, healthcare and other critical sectors face the increasingly present threat of cyber attacks to their industrial control systems (ICS). Advanced persistent threat (APT) groups have the resources and support to mount attacks that are complex, orchestrated, and ever-more sophisticated. Operators of critical infrastructure face the critical task of continually safeguarding key OT and IT systems from this kind of compromise and damage.

The 2nd ICS/SCADA Cybersecurity Symposium, June 16-18, 2026 in Chicago, is focused on providing real-world preparation to critical infrastructure operators for successfully dealing with a continually evolving range of cybersecurity threats. Emerging technologies and strategies are examined in detail, with the aim of helping asset owners meet the challenges that confront their unique type of ICS/SCADA infrastructures on a daily basis.

If your organization is faced with safeguarding critical infrastructure from challenges such as ransomware and nation-state APT actors, this is a must-attend opportunity to network one-on-one with key colleagues, industry thought leaders and solution providers.

Chicago, Illinois, USA; June 16th -18th 2026

More details can be found on the following website:

https://ics-scada-symposium.com/

3. Critical systems security incidents

Polish Security Agency Reports ICS Breaches at Five Water Treatment Plants

The latest report from Poland's Internal Security Agency (ABW) delineates a sobering shift in the regional cyber-threat landscape, documenting a significant escalation in attacks targeting Industrial Control Systems (ICS) and Operational Technology (OT) infrastructure throughout 2024 and 2025. This period marks a strategic pivot by state-sponsored actors from traditional espionage toward the deliberate physical disruption of municipal services, with the Polish water sector emerging as a primary and highly vulnerable target.

A central revelation of the report concerns a series of direct intrusions into water treatment facilities across several Polish municipalities, including Jabłonna Lacka, Szczytno, Małdyty, Tolkmicko, and Sierakowo. In the most severe incidents recorded in 2025, threat actors moved beyond mere unauthorized access, gaining the capability to modify the operational parameters of critical equipment. This level of control represents a direct risk to public safety and the continuity of the water supply. While a major city-wide supply failure was successfully thwarted in August 2025, the ABW confirms that the potential for a catastrophic public health crisis was a tangible reality during these breaches.

The technical analysis provided by the ABW identifies a recurring and systemic failure in "security hygiene" within the OT environment. The two primary vectors utilized by attackers were weak password policies and the exposure of ICS devices directly to the public internet. These vulnerabilities are not new, yet their persistence allowed attackers to bypass security layers with alarming ease. The report notes that these same weaknesses were recently exploited in Russia-linked campaigns against Polish energy facilities, suggesting a coordinated methodology used by adversaries to probe and penetrate various sectors of Poland's national infrastructure.

Furthermore, the threat extends beyond water management to include wastewater treatment, waste incineration, and the broader industrial supply chain. The ABW highlights a sophisticated approach to supply chain attacks, where investigators found that attackers focused on exfiltrating contract data, project documentation, and authentication credentials. This information-gathering phase is designed to facilitate "downstream" access, allowing actors to move laterally from a private contractor into the sensitive internal networks of government and municipal utilities.

Regarding attribution, the ABW's findings point toward a complex ecosystem where "hacktivist" personas serve as a front for foreign intelligence services. The report explicitly identifies Russian-linked Advanced Persistent Threat (APT) groups, specifically APT28 (Fancy Bear) and APT29 (Cozy Bear), alongside the Belarusian-linked UNC1151, as the primary perpetrators. These groups are known for their high degree of technical sophistication and their alignment with the geopolitical objectives of their respective states. The targeting of Polish infrastructure is characterized not merely as random cybercrime, but as a deliberate instrument of statecraft intended to undermine public trust and weaken the national resilience of a key NATO ally.

The source is available at the following link:

https://www.securityweek.com/polish-security-agency-reports-ics-breaches-at-five-water-treatment-plants/

4. Book recommendation

Hacking OT Networks: A Practical Guide To Pentesting Industrial Networks

Hacking OT Networks: A Practical Guide to Pentesting Industrial Networks moves beyond isolated exploits and theoretical models to cover the messy reality of OT security. It tracks the full lifecycle of a real-world assessment, starting in the enterprise, crossing the IT/OT boundary, navigating the DMZ, and ending in the process control network.

Born from hundreds of engagements across electric power, water, manufacturing, and oil & gas, this guide prioritizes tradecraft over tools. You won't just run commands; you will learn how adversaries chain together misconfigurations, credential reuse, and weak architectures to reach critical assets without needing zero-day exploits.

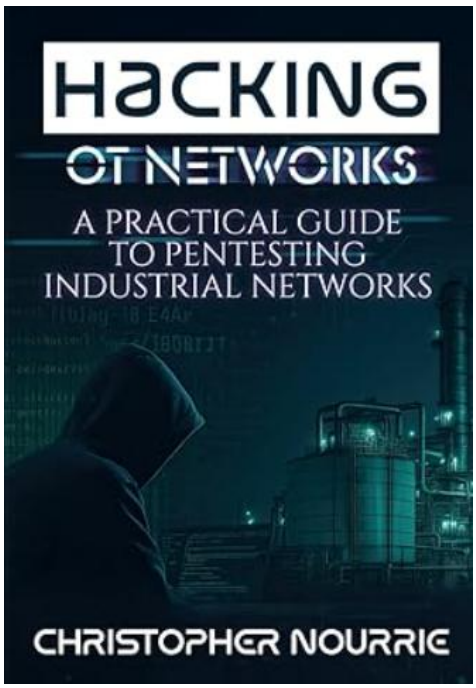
Crucially, this book covers the consulting side of the job, the part technical guides usually ignore. It teaches you how to scope responsibly, collaborate with plant engineers, and demonstrate risk without accidentally tripping a breaker or halting production. The goal isn't just to get access; it's to translate that access into business value.

Author/Editor: Christopher Nourrie (Author)

Year of issue: 2026

The book is available at the following link:

https://www.amazon.com/Hacking-Networks-Practical-Pentesting-Industrial/dp/B0GHHJ9Y3D



5. Critical systems security news selection

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

1. **Fortinet flags 'industrial scale' cybercrime scale driven by continuous, machine-speed attacks and automated exploitation**
2. **Cybersecurity Experts Unimpressed With CISA OT Guidance**
3. **Hundreds of Internet-Facing VNC Servers Expose ICS/OT**
4. **World's First AI-Driven Cyberattack Couldn't Breach OT Systems**
5. **AI Era Raises Stakes for IT-OT Integration Security**
6. **Taiwan Bullet Train Hack Highlights Cybersecurity Gaps in Rail Systems**
7. **US probes automatic tank gauge system breaches, exposing OT risks across critical infrastructure**
8. **Verizon DBIR finds vulnerability exploitation overtakes stolen credentials as top breach entry point for critical infrastructure**
9. **Real-World ICS Security Tales From the Trenches**
10. **Patch Now: Critical Flaw in OT Robot OS Gives Attackers Control**
11. **Water, the Soft Underbelly of Critical Infrastructure**
12. **Zero trust in OT moves beyond identity as industrial operators prioritize visibility, segmentation, operational resilience**
13. **AI-powered penetration testing for industrial systems moves from experimental concept to practical toolkit**
14. **Oil shipments, drone makers, and a poisoned code library targeted in recent APT campaigns**

Fortinet flags 'industrial scale' cybercrime scale driven by continuous, machine-speed attacks and automated exploitation

Fortinet released its 2026 Global Threat Landscape Report from FortiGuard Labs, framing cybercrime in 2025 as an industrialized, system-level operation rather than a series of isolated campaigns. Drawing exclusively on FortiGuard telemetry, the report captures a threat environment defined by continuous, machine-speed activity, where exposure is persistently mapped, validated, and exploited without reliance on traditional campaign cycles or manual intervention. The data shows attackers operating across an end-to-end lifecycle, compressing timelines and scaling operations through automation and coordinated tooling. …

Source and more information:

Fortinet flags 'industrial scale' cybercrime scale driven by continuous, machine-speed attacks and automated exploitation - Industrial Cyber

Cybersecurity Experts Unimpressed With CISA OT Guidance

New guidance from the U.S. Cybersecurity and Infrastructure Security Agency on adapting zero trust security principles for operational technology is fine as far as it goes, but is pretty high-level and ignores or fudges a couple of key questions, say executives and experts.

"This is a great guide that takes the right direction, but it dodges the hardest question, which is who pays for it?" said Tatyana Bolton, executive director of the Operational Technology Cybersecurity Coalition, an industry group that represents OT equipment makers, owners and operators and security vendors.

"The technical thinking is sound," she told ISMG, "But the vast majority of critical infrastructure owners and operators like water utilities, rural [electricity] co-ops, or small ports simply can't afford to implement." …

Source and more information:

Cybersecurity Experts Unimpressed With CISA OT Guidance

Hundreds of Internet-Facing VNC Servers Expose ICS/OT

Millions of remote access RDP and VNC servers are exposed to the internet, and hundreds of them may provide access to industrial control systems (ICS) and other operational technology (OT), according to research by Forescout.

RDP (Remote Desktop Protocol) and VNC (Virtual Network Computing) are widely used for remote access, but they should not be exposed directly to the open internet without a secure gateway.

A Shodan search shows roughly 1.8 million RDP and 1.6 million VNC servers exposed on the internet, a majority in China and the United States. Forescout has determined that the majority are honeypots, ISPs, and hosting providers, but its researchers still found 91,000 RDP and 29,000 VNC servers that could be linked to specific industries. …

Source and more information:

Hundreds of Internet-Facing VNC Servers Expose ICS/OT - SecurityWeek

World's First AI-Driven Cyberattack Couldn't Breach OT Systems

The most sophisticated AI-integrated campaign to date hit a brick wall in the form of a SCADA login screen.

A small, unknown band of hackers pulled off history's first recorded, truly artificial intelligence-directed cyberattack earlier this year, stealing troves of data from the government of Mexico

in the process. Yet when the enterprising ne'er-do-wells tried bridging the gap from IT to OT systems, the AI had no luck. …

Source and more information:

AI-Driven Cyberattack on Mexico Couldn't Breach OT Systems

AI Era Raises Stakes for IT-OT Integration Security

Manufacturing organizations are accelerating IT-OT integration to support smart manufacturing, predictive maintenance and data analytics. That convergence has increased cyber risk across operational technology environments, especially as artificial intelligence-driven attacks grow more sophisticated.

Ambarish Kumar Singh, CISO at India-based manufacturer Godrej, said many organizations depend on remote access for original equipment manufacturer troubleshooting, which creates additional exposure when security controls are weak. …

Source and more information:

AI Era Raises Stakes for IT-OT Integration Security

Taiwan Bullet Train Hack Highlights Cybersecurity Gaps in Rail Systems

A Taiwanese student experimenting with software-defined radio technology shut down three bullet trains for nearly an hour, leading to an anti-terrorism response.

The communications and monitoring platforms for rail networks has come under scrutiny following the recent "hacking" of a Taiwanese railway operators' radio system, which led to the emergency stoppage of three high-speed bullet trains for nearly an hour.

On April 5, a 23-year-old train enthusiast used a software-defined radio set up and hardware bought online to spoof a general alarm, or GA, alert to the operations center of Taiwan High Speed Rail (THSR). The company issued orders for emergency braking to the three high-speed trains in the vicinity of the signal, resulting in a 48-minute delay in service. …

Source and more information:

Taiwan Bullet Train Hack Shows Cybersecurity Gaps in Rail Systems

US probes automatic tank gauge system breaches, exposing OT risks across critical infrastructure

U.S. officials are investigating a series of cyber intrusions targeting automatic tank gauge systems used to monitor fuel levels at gas stations across multiple states, with Iran emerging as a leading suspect, according to a CNN report citing officials and cybersecurity experts. The attackers allegedly exploited internet-connected tank monitoring systems that lacked

password protection, allowing them in some cases to manipulate displayed fuel readings, though officials said the actual fuel levels inside storage tanks were not altered.

While investigators said the breaches did not cause physical damage or injuries, the incidents have raised broader concerns about the cybersecurity of operational technology embedded across critical infrastructure. Officials and private-sector experts warned that unauthorized access to automatic tank gauge systems could theoretically be used to conceal fuel leaks or create operational confusion. …

Source and more information:

US probes automatic tank gauge system breaches, exposing OT risks across critical infrastructure - Industrial Cyber

Verizon DBIR finds vulnerability exploitation overtakes stolen credentials as top breach entry point for critical infrastructure

New data from Verizon 2026 Data Breach Investigations Report (DBIR) underscores growing cyber risk for critical infrastructure and industrial sectors, as exploitation of software vulnerabilities overtook stolen credentials for the first time to become the leading breach entry point, accounting for 31% of incidents. The report warns that AI-assisted attacks are dramatically compressing the time between vulnerability disclosure and exploitation, reducing defenders' response windows from months to hours.

Verizon also found that third-party and supply chain-related breaches surged, while mobile-focused social engineering attacks achieved a 40% higher success rate than traditional phishing campaigns, trends that could have significant implications for manufacturing, utilities, transportation, and other OT (operational technology)-heavy environments increasingly exposed through connected systems and external vendor ecosystems. …

Source and more information:

Verizon DBIR finds vulnerability exploitation overtakes stolen credentials as top breach entry point for critical infrastructure - Industrial Cyber

Real-World ICS Security Tales From the Trenches

Industrial control systems (ICS) and operational technology (OT) environments are often described as quiet, highly controlled worlds. In reality, they contain a range of risks, unexpected configurations, and operational complexities that are difficult to fully uncover through standard penetration testing or conventional risk assessments.

SecurityWeek spoke with several ICS security experts and companies about their most memorable experiences in the field. These are not theoretical scenarios or lab simulations — they are real situations they encountered while working directly with organizations. …

Source and more information:

Real-World ICS Security Tales From the Trenches - SecurityWeek

Patch Now: Critical Flaw in OT Robot OS Gives Attackers Control

A critical command injection vulnerability in the operating system (OS) for collaborative robots used across operational technology (OT) environments allows an unauthenticated attacker to execute commands on the system. Exploiting the flaw could threatens the integrity of the system and potentially the safety of those interacting with it.

Danish company Universal Robots has patched the vulnerability, tracked as CVE-2026-8153 and found in the Dashboard Server interface of Universal Robots PolyScope 5. The flaw exists because the Dashboard Server accepts user-controlled input and passes it to the underlying OS without proper neutralization of special elements, according to a company security advisory. ...

Source and more information:

Patch Now: Critical Flaw in OT Robot OS Gives Attackers Control

Water, the Soft Underbelly of Critical Infrastructure

America's water utilities are the nation's most cyber-vulnerable critical service sector, but their cybersecurity is overseen and supported by an ill-fitting patchwork of government agencies and most lack the resources to meet the threat they face, a congressional panel heard Thursday.

"The far-reaching implications of a successful cyberattack that disrupts water treatment and distribution systems cannot be overstated," declared Rep. Scott Franklin, R-Fla., chairman of the environment subcommittee of the House Science, Space and Technology Committee. "A cyberattack on water systems could lead to widespread ramifications across different sectors, including chemicals, manufacturing and energy ... It can also severely impact emergency response operations, hospitals, firefighters and food production" (See: Russian Attacks on Polish Water Utilities Use Fear as Weapon). ...

Source and more information:

Water, the Soft Underbelly of Critical Infrastructure

Zero trust in OT moves beyond identity as industrial operators prioritize visibility, segmentation, operational resilience

With increasing levels of connectivity within industrial environments, traditional notion of trusted users, devices, and networks being fundamentally safe is being challenged by the current wave of cyber threats and attacks. Several PLCs, sensors, and industrial controllers continue to use shared credentials, weak authentication, and implicit trust between systems,

while other OT assets cannot support modern forms of identity management, use unsupported firmware, or exist outside the vendor's software lifecycle.

It is becoming common knowledge amongst security professionals that zero trust in an OT environment must not start with strict enforcement policies but rather with visibility, asset discovery, segmentation and improved knowledge of how industrial operations and systems communicate. Forrester identified that visibility, isolation, and control were established as foundational concepts for the protection of connected OT and IoT environments. Such concepts can be seen as the building blocks of a phased approach towards asset management, segmentation, and identity. …

Source and more information:

Zero trust in OT moves beyond identity as industrial operators prioritize visibility, segmentation, operational resilience - Industrial Cyber

AI-powered penetration testing for industrial systems moves from experimental concept to practical toolkit

Researcher Isiah Jones published a broader 'Security Methodology' initiative that consolidates projects such as ICSOTPentest, AIpentest 3.1, AI-driven OT security demonstrations, command-line scripts, testing templates, research papers, and ICS (industrial control system)-focused security resources into a public framework hosted through GitHub repositories. The project positions itself as a practical resource hub for penetration testing, assessment workflows, and applied security research spanning industrial systems, IoT, and AI-driven cybersecurity experimentation.

Among the efforts drawing attention are demonstrations and toolsets shared through LinkedIn, GitHub, YouTube, and other social media platforms associated with the @aicyberiot profile, including the ICSOTPentest toolkit and the AIpentest 3.1 cybersecurity demonstration focused on AI-assisted security testing. The program emphasizes an important connection between AI-assisted security analyses and OT security in general. A couple of the linked projects and demonstrations bring about AI-enabled detection, automation, and threat analysis for cyber-physical systems, reflecting growing industry interest in applying AI to industrial threat detection, security validation, and cyber-physical risk analysis. …

Source and more information:

AI-powered penetration testing for industrial systems moves from experimental concept to practical toolkit - Industrial Cyber

Oil shipments, drone makers, and a poisoned code library targeted in recent APT campaigns

Geopolitical pressure drove much of the state-sponsored cyber activity recorded between October 2025 and March 2026, according to ESET's latest APT Activity Report. Espionage

groups aligned with China, North Korea, Russia, and Iran adjusted their targets to match the economic and security concerns of their governments.

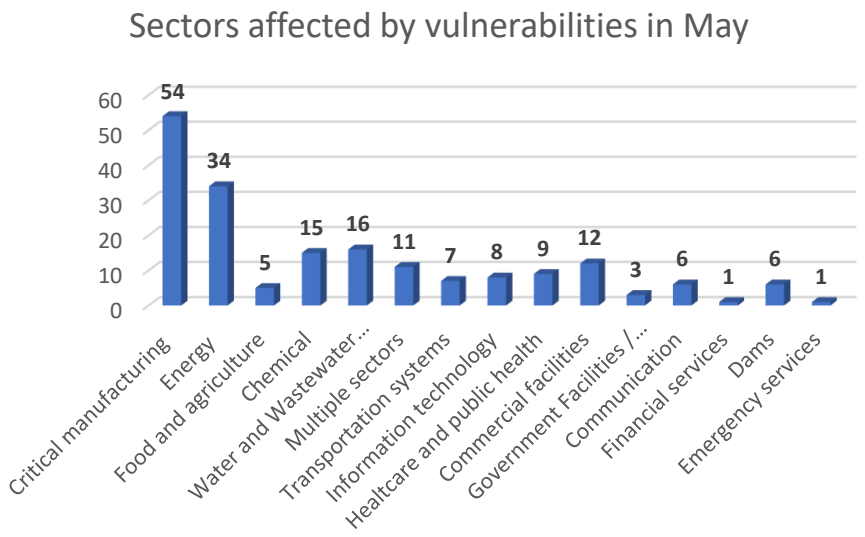
"In Asia, the campaigns primarily focused on governmental organizations, strategic industries, and advanced technology sectors. In the Middle East, Israel remained the principal focus of Iran-aligned and Iran-linked activities, with targets ranging from organizations affected by espionage intrusions to device manufacturers hit by destructive tooling," Jean-Ian Boutin, Director of Threat Research at ESET, explained. …

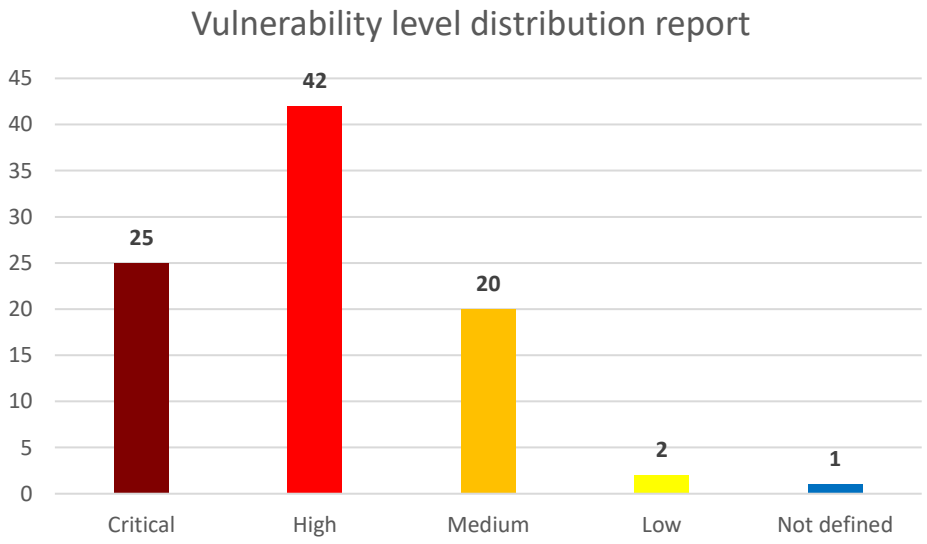
Source and more information:

Oil shipments, drone makers, and a poisoned code library targeted in recent APT campaigns - Help Net Security

6. Critical systems vulnerabilities

In May 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-26-148-01: **MacGregor Voyage Data Recorder (VDR) G4e**

High level vulnerabilities: Use of Default Credentials, Insufficiently Protected Credentials, Use of Password Hash With Insufficient Computational Effort, Use of Hard-coded Credentials, Files or Directories Accessible to External Parties.

MacGregor Voyage Data Recorder (VDR) G4e | CISA

ICSA-26-148-02: **Jinan USR IOT Technology Limited (PUSR) USR-W610 RS232/485 to Wi-Fi/Ethernet Converter**

Critical level vulnerability: Use of Hard-coded Credentials.

Jinan USR IOT Technology Limited (PUSR) USR-W610 RS232/485 to Wi-Fi/Ethernet Converter | CISA

ICSA-26-148-03: **ABB EIBPORT**

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

ABB EIBPORT | CISA

ICSA-26-148-04: **ABB Busch-Welcome 2 Wire Door Opener Actuator**

Medium level vulnerability: Active Debug Code.

ABB Busch-Welcome 2 Wire Door Opener Actuator | CISA

ICSA-26-148-05: **CP Plus 8 Ch. Network Video Recorder**

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

CP Plus 8 Ch. Network Video Recorder | CISA

ICSA-26-148-06: **KMW CCTV Security Cameras**

Critical level vulnerability: Unverified Password Change.

KMW CCTV Security Cameras | CISA

ICSA-26-148-07: **Schnieider Electric EcoStruxure Machine Expert HVAC**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Schnieider Electric EcoStruxure Machine Expert HVAC | CISA

ICSA-26-148-08: **XCharge C6**

Critical level vulnerabilities: Download of Code Without Integrity Check, Stack-based Buffer Overflow, Initialization of a Resource with an Insecure Default.

XCharge C6 | CISA

ICSMA-26-148-01: **Fourth Frontier Frontier X Mobile Application, Frontier X2**

High level vulnerability: Missing Authentication for Critical Function.

Fourth Frontier Frontier X Mobile Application, Frontier X2 | CISA

ICSA-20-212-04: **Mitsubishi Electric Factory Automation Engineering Products (Update L)**

High level vulnerability: Unquoted Search Path or Element.

Mitsubishi Electric Factory Automation Engineering Products (Update L) | CISA

ICSA-26-146-03: **ABB Ability Zenon Remote Transport Vulnerability (Update A)**

High level vulnerability: Missing Authentication for Critical Function.

ABB Ability Zenon Remote Transport Vulnerability (Update A) | CISA

ICSA-26-146-01: **ABB Terra AC**

Medium level vulnerability: Heap-based Buffer Overflow.

ABB Terra AC | CISA

ICSA-26-146-02: **ABB AC500 V2**

Medium level vulnerability: Buffer Over-read.

ABB AC500 V2 | CISA

ICSA-26-146-03: **ABB AbilityTM Zenon Remote Transport Vulnerability**

High level vulnerability: Missing Authentication for Critical Function.

ABB AbilityTM Zenon Remote Transport Vulnerability | CISA

ICSA-26-146-04: **ABB B&R Automation Runtime DoS Vulnerability in System Diagnostics Manager**

Critical level vulnerability: Improper Resource Locking.

ABB B&R Automation Runtime DoS Vulnerability in System Diagnostics Manager (SDM) | CISA

ICSA-26-146-05: **ABB Ability Camera Connect**

Critical level vulnerabilities: Heap-based Buffer Overflow, Integer Underflow (Wrap or Wraparound), Out-of-bounds Write, Uncontrolled Search Path Element, Integer Overflow or Wraparound, Off-by-one Error, Out-of-bounds Read, Double Free, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use After Free.

ABB Ability Camera Connect | CISA

ICSA-26-146-06: **ABB LVS MConfig**

High level vulnerability: Cleartext Storage of Sensitive Information in Memory.

ABB LVS MConfig | CISA

ICSMA-26-146-01: **Eppendorf BioFlo 320**

Critical level vulnerability: Use of Hard-coded Password.

Eppendorf BioFlo 320 | CISA

ICSA-25-259-01: **Schneider Electric Multiple Altivar Process Drives and Communication Modules (Update B)**

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

Schneider Electric Altivar Products, ATVdPAC Module, ILC992 InterLink Converter (Update B) | CISA

ICSA-26-141-01: **Hitachi Energy GMS600**

Medium level vulnerability: Observable Discrepancy.

Hitachi Energy GMS600 | CISA

ICSA-26-141-02: **ABB B&R PCs**

High level vulnerabilities: Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Loop with Unreachable Exit Condition ('Infinite Loop'), Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).

ABB B&R PCs | CISA

ICSA-26-141-03: **ABB B&R Automation Studio**

Critical level vulnerabilities: Numeric Truncation Error, Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, NULL Pointer Dereference, Incorrect User Management, Use After Free, Integer Overflow or Wraparound, Improper Check for Unusual or Exceptional Conditions, Uncontrolled Recursion, Out-of-bounds Read, Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

ABB B&R Automation Studio | CISA

ICSA-26-141-04: **ABB B&R Automation Runtime**

Medium level vulnerabilities: Generation of Predictable Numbers or Identifiers, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Neutralization of Formula Elements in a CSV File.

ABB B&R Automation Runtime | CISA

ICSA-26-141-05: **ABB Terra AC Wallbox**

Medium level vulnerabilities: Heap-based Buffer Overflow, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Stack-based Buffer Overflow.

ABB Terra AC Wallbox | CISA

ICSA-26-022-01: **Schneider Electric EcoStruxure Process Expert (Update A)**

High level vulnerability: Incorrect Default Permissions.

Schneider Electric EcoStruxure Process Expert (Update A) | CISA

ICSA-25-133-04: **ABB Automation Builder (Update A)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

ABB Automation Builder (Update A) | CISA

SSA-921111: **Two File Parsing Vulnerabilities in Solid Edge Before Version SE226 Update 5 (Update: 1.1.)**

High level vulnerabilities: Access of Uninitialized Pointer, Stack-based Buffer Overflow.

SSA-921111

SSA-975644: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Verification of Source of a Communication Channel, Use of Externally-Controlled Format String, Authentication Bypass Using an Alternate Path or Channel.

SSA-975644

SSA-904646: **Sensitive Data Exposure Vulnerability in SIPROTEC 5 Devices (Update: 1.1.)**

Medium level vulnerability: Use of GET Request Method With Sensitive Query Strings.

SSA-904646

SSA-827968: **Vulnerability in Nozomi Guardian/CMC Before V26.2.0 on RUGGEDCOM APE1808 Devices (Update: 1.2.)**

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

SSA-827968

SSA-723487: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products (Update: 1.9.)**

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

SSA-723487

SSA-452276: **Eval Injection Vulnerability in SIMATIC S7-1500 (Update: 1.3.)**

Critical level vulnerability: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection').

SSA-452276

SSB-295699: **Configuration of Microsoft Defender Antivirus for SIMATIC PCS 7 and SIMATIC PCS neo (Update: 1.1.)**

Not defined

SSB-295699

SSA-280834: **Improper OpenVPN Credential Validation Vulnerability in SCALANCE M-800 and SC-600 Families (Update: 1.1.)**

Medium level vulnerability: Partial String Comparison.

SSA-280834

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1 (Update: 2.2.)**

High level vulnerabilities: Multiple.

SSA-265688

SSA-216014: **Vulnerabilities in EFI variable of SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs (Update: 1.5.)**

High level vulnerability: Protection Mechanism Failure.

SSA-216014

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: 1.5.)**

High level vulnerabilities: Multiple.

SSA-082556

SSA-001536: **Authorization Bypass Vulnerability in Siemens Industrial Edge Devices (Update: 1.1.)**

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

SSA-001536

ICSA-26-139-01: **ABB CoreSense HM and CoreSense M10**

High level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

ABB CoreSense HM and CoreSense M10 | CISA

ICSA-26-139-02: **Siemens RUGGEDCOM APE1808 Devices**

Critical level vulnerability: Out-of-bounds Write.

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-26-139-03. **ScadaBR**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Cross-Site Request Forgery (CSRF), Use of Hard-coded Credentials.

ScadaBR | CISA

ICSA-26-139-04: **ZKTeco CCTV Cameras**

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

ZKTeco CCTV Cameras | CISA

ICSA-26-139-05: **Kieback & Peter DDC Building Controllers**

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

Kieback & Peter DDC Building Controllers | CISA

ICSA-24-177-01: **ABB 800xA Base (Update A)**

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

ABB 800xA Base (Update A) | CISA

ICSA-25-196-02: **ABB RMC-100 (Update A)**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Stack-based Buffer Overflow.

ABB RMC-100 (Update A) | CISA

ICSA-26-134-01: **Siemens gWAP**

High level vulnerability: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting').

Siemens gWAP | CISA

ICSA-26-134-02: **Siemens Ruggedcom Rox**

Medium level vulnerability: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection').

Siemens Ruggedcom Rox | CISA

ICSA-26-134-03: **Siemens Solid Edge**

High level vulnerabilities: Access of Uninitialized Pointer, Stack-based Buffer Overflow.

Siemens Solid Edge | CISA

ICSA-26-134-04: **Siemens Teamcenter**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Use of Hard-coded Credentials.

Siemens Teamcenter | CISA

ICSA-26-134-05: **Siemens Simcenter Femap**

High level vulnerability: Heap-based Buffer Overflow.

Siemens Simcenter Femap | CISA

ICSA-26-134-06: **Siemens Industrial Devices**

High level vulnerability: NULL Pointer Dereference.

Siemens Industrial Devices | CISA

ICSA-26-134-07: **Siemens SIMATIC**

High level vulnerability: Initialization of a Resource with an Insecure Default.

Siemens SIMATIC | CISA

ICSA-26-134-08: **Siemens Siemens ROS#**

Critical level vulnerability: Relative Path Traversal.

Siemens Siemens ROS# | CISA

ICSA-26-134-09: **Siemens Opcenter RDnL**

High level vulnerability: Missing Authentication for Critical Function.

Siemens Opcenter RDnL | CISA

ICSA-26-134-10: **Siemens SIMATIC CN 4100**

Critical level vulnerabilities: NULL Pointer Dereference, Reachable Assertion, Use After Free, Out-of-bounds Write, Integer Overflow or Wraparound, Allocation of Resources Without Limits or Throttling, Out-of-bounds Read, Covert Timing Channel, Stack-based Buffer Overflow, Inefficient Algorithmic Complexity, Missing Release of Memory after Effective Lifetime, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Improper Locking, Uncontrolled Recursion, Buffer Access with Incorrect Length Value, Race Condition within a Thread, Missing Synchronization, Use of Uninitialized Resource, Double Free, Missing Release of Resource after Effective Lifetime, Loop with Unreachable Exit Condition ('Infinite Loop'), Improper Update of Reference Count, Improper Control of a Resource Through its Lifetime, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Unexpected Status Code or Return Value, Divide By Zero, Improper Validation of Specified Index, Position, or Offset in Input, Comparison Using Wrong Factors, Observable Timing Discrepancy, Improper Validation of Syntactic Correctness of Input, Deadlock, Signal Handler Race Condition, Improper Following of Specification by Caller, Improper Check for Dropped Privileges, Transmission of Private Resources into a New Sphere ('Resource Leak'), Improper Resource Shutdown or Release, Improper Access Control, Exposure of Sensitive Information to an Unauthorized Actor, Relative Path Traversal, Improper Neutralization of Escape, Meta, or Control Sequences, Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade'), Uncontrolled Resource Consumption, Improper

Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authentication for Critical Function, Improper Check for Unusual or Exceptional Conditions.

Siemens SIMATIC | CISA

ICSA-26-134-11: **Siemens Ruggedcom Rox**

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

Siemens Ruggedcom Rox | CISA

ICSA-26-134-12: **Siemens Ruggedcom Rox**

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

Siemens Ruggedcom Rox | CISA

ICSA-26-134-13: **Siemens SIPROTEC 5**

Medium level vulnerability: Small Space of Random Values.

Siemens SIPROTEC 5 | CISA

ICSA-26-134-14: **Siemens SENTRON 7KT PAC1261 Data Manager**

Critical level vulnerability: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling').

Siemens SENTRON 7KT PAC1261 Data Manager | CISA

ICSA-26-134-15: **Siemens SIMATIC S7 PLC Web Server**

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

Siemens SIMATIC S7 PLC Web Server | CISA

ICSA-26-134-16: **Siemens Ruggedcom Rox**

Critical level vulnerabilities: Uncontrolled Recursion, Integer Underflow (Wrap or Wraparound), Out-of-bounds Write, Out-of-bounds Read, Improper Input Validation, Heap-based Buffer Overflow, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Use After Free, Improper Validation of Syntactic Correctness of Input, Improper Control of a Resource Through its Lifetime, Integer Overflow or Wraparound, Incorrect Calculation of Buffer Size, Use of Weak Hash, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Stack-based Buffer Overflow, Expired Pointer Dereference.

Siemens Ruggedcom Rox | CISA

ICSA-26-134-17: **Universal Robots Polyscope 5**

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

Universal Robots Polyscope 5 | CISA

ICSA-26-057-06: **SWTCH EV swtchenergy.com (Update A)**

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

SWTCH EV swtchenergy.com (Update A) | CISA

ICSA-26-132-01: **Fuji Electric Tellus**

High level vulnerability: Exposed Dangerous Method or Function.

Fuji Electric Tellus | CISA

ICSA-26-132-02: **Subnet Solutions PowerSYSTEM Center**

High level vulnerabilities: Incorrect Authorization, Improper Neutralization of CRLF Sequences ('CRLF Injection').

Subnet Solutions PowerSYSTEM Center | CISA

ICSA-26-132-03: **ABB AC500 V3 Multiple Vulnerabilities**

High level vulnerabilities: Direct Request ('Forced Browsing'), Incorrect Permission Assignment for Critical Resource, NULL Pointer Dereference.

ABB AC500 V3 Multiple Vulnerabilities | CISA

ICSA-26-132-04: **ABB Automation Builder Gateway for Windows**

Medium level vulnerability: Initialization of a Resource with an Insecure Default.

ABB Automation Builder Gateway for Windows | CISA

ICSA-26-132-05: **ABB AC500 V3 Stack buffer overflow in Cryptographic Message Syntax**

Critical level vulnerability: Out-of-bounds Write.

ABB AC500 V3 Stack Buffer Overflow in Cryptographic Message Syntax | CISA

ICSA-26-132-06: **ABB WebPro SNMP Card PowerValue**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Incorrect Implementation of Authentication Algorithm, Insufficient Session Expiration.

ABB WebPro SNMP Card PowerValue Multiple Vulnerabilities | CISA

ICSA-25-329-01: **Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share (Update A)**

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

Ashlar-Vellum Cobalt, Xenon, Argon, Lithium, Cobalt Share (Update A) | CISA

ICSA-26-127-01: **Maxhub Pivot**

High level vulnerability: Use of a Broken or Risky Cryptographic Algorithm.

MAXHUB Pivot Client Application | CISA

ICSA-24-331-03: **Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs (Update A)**

High level vulnerabilities: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Use of Hard-coded Credentials, Insufficiently Protected Credentials.

Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs (Update A) | CISA

ICSA-26-113-06: **Intrado 911 Emergency Gateway (EGW) (Update A)**

Critical level vulnerability: Path Traversal: '.../...//'.

Intrado 911 Emergency Gateway (EGW) (Update A) | CISA

ICSMA-18-219-01: **Medtronic MyCareLink 24950 Patient Monitor (Update A)**

Medium level vulnerabilities: Insufficient Verification of Data Authenticity, Cleartext Storage in a File or on Disk.

Medtronic MyCareLink 24950 Patient Monitor (Update A) | CISA

ICSMA-25-205-01: **Medtronic MyCareLink Patient Monitor (Update A)**

Medium level vulnerabilities: Cleartext Storage of Sensitive Information, Empty Password in Configuration File, Deserialization of Untrusted Data, Cleartext Storage in a File or on Disk, Improper Physical Access Control.

Medtronic MyCareLink Patient Monitor (Update A) | CISA

ICSA-26-125-01: **Hitachi Energy PCM600**

Low level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Hitachi Energy PCM600 | CISA

ICSA-26-125-02: **ABB B&R PVI**

Medium level vulnerability: Insertion of Sensitive Information into Log File.

ABB B&R PVI | CISA

ICSA-26-125-03: **ABB B&R Automation Runtime**

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

ABB B&R Automation Runtime | CISA

ICSA-26-125-04: **ABB B&R Automation Studio**

High level vulnerability: Improper Certificate Validation.

ABB B&R Automation Studio | CISA

ICSA-26-125-05: **Johnson Controls CEM AC2000**

High level vulnerability: Uncontrolled Search Path Element.

Johnson Controls CEM AC2000 | CISA

ICSA-23-227-01: **Schneider Electric EcoStruxure Control Expert and Modicon M340, Momentum, MC80, M580 and M580 CPU Safety (Update A)**

High level vulnerability: Authentication Bypass by Capture-replay.

Schneider Electric EcoStruxure Control Expert and Modicon M340, Momentum, MC80, M580 and M580 CPU Safety (Update A) | CISA

ICSA-24-319-06: **Hitachi Energy MSM (Update A)**

High level vulnerabilities: Missing Release of Resource after Effective Lifetime, Loop with Unreachable Exit Condition ('Infinite Loop').

Hitachi Energy MSM (Update A) | CISA

ICSA-26-120-01 **ABB System 800xA, Symphony Plus IEC 61850**

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

ABB System 800xA, Symphony Plus IEC 61850 | CISA

ICSA-26-120-02 **ABB PCM600**

Low level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

ABB PCM600 | CISA

ICSA-26-120-03 **ABB Edgenius Management Portal**

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

ABB Edgenius Management Portal | CISA

ICSA-26-120-04 **ABB Ability OPTIMAX**

High level vulnerability: Incorrect Implementation of Authentication Algorithm.

ABB Ability OPTIMAX | CISA

ICSA-26-120-05 **ABB AWIN Gateways**

High level vulnerabilities: Authentication Bypass by Capture-replay, Missing Authentication for Critical Function.

ABB AWIN Gateways | CISA

ICSA-26-120-06 **ABB Ability Symphony Plus Engineering**

High level vulnerabilities: Integer Overflow or Wraparound, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Time-of-check Time-of-use (TOCTOU) Race Condition, Privilege Dropping / Lowering Errors.

ABB Ability Symphony Plus Engineering | CISA

ICSA-25-128-03 **Mitsubishi Electric Multiple FA Products (Update C)**

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

Mitsubishi Electric Multiple FA Products (Update C) | CISA

ICSA-26-062-01 **Mitsubishi Electric MELSEC iQ-F Series EtherNet/IP module and Ethernet Module (Update A)**

High level vulnerabilities: Always-Incorrect Control Flow Implementation, Improper Resource Shutdown or Release.

Mitsubishi Electric MELSEC iQ-F Series EtherNet/IP module and Ethernet module (Update A) | 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 May:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-31431 Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability;
CVE-2026-0300 Palo Alto Networks PAN-OS Out-of-bounds Write Vulnerability;
CVE-2026-6973 Ivanti Endpoint Manager Mobile (EPMM) Improper Input Validation Vulnerability;
CVE-2026-42208 BerriAI LiteLLM SQL Injection Vulnerability;
CVE-2026-20182 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability;
CVE-2026-42897 Microsoft Exchange Server Cross-Site Scripting Vulnerability;
CVE-2008-4250 Microsoft Windows Buffer Overflow Vulnerability;
CVE-2009-1537 Microsoft DirectX NULL Byte Overwrite Vulnerability;
CVE-2009-3459 Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability;
CVE-2010-0249 Microsoft Internet Explorer Use-After-Free Vulnerability;
CVE-2010-0806 Microsoft Internet Explorer Use-After-Free Vulnerability;
CVE-2026-41091 Microsoft Defender Elevation of Privilege Vulnerability;
CVE-2026-45498 Microsoft Defender Denial of Service Vulnerability;
CVE-2025-34291 Langflow Origin Validation Error Vulnerability;
CVE-2026-34926 Trend Micro Apex One (On-Premise) Directory Traversal Vulnerability;
CVE-2026-9082 Drupal Core SQL Injection Vulnerability;
CVE-2026-48172 LiteSpeed cPanel Plugin Privilege Escalation Vulnerability;
CVE-2026-8398 Daemon Tools Lite Embedded Malicious Code Vulnerability;
CVE-2026-45321 TanStack Unspecified Vulnerability;
CVE-2026-48027 Nx Console Embedded Malicious Code Vulnerability;

Links and more information:

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 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 Seven 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 Three Known Exploited Vulnerabilities to Catalog | CISA

CI Fortify: Strengthening Resilience Across Critical Infrastructure

CISA urges critical infrastructure operators to defend against disruptive cyberattacks with proactive isolation and recovery planning.

U.S. critical infrastructure (CI) operators face constant intrusion attempts from nation-state cyber threat actors. These adversaries aim for more than espionage. To win a wider geopolitical conflict:

- *They have successfully pre-positioned across critical infrastructure to disrupt and destroy the operational technology (OT) running the United States.*
- *They could leverage access to telecommunications infrastructure to take out phone and internet services.*

CI owners and operators must fortify their systems to allow vital services in the United States to sustain essential operations during a geopolitical conflict. Investing in isolation and recovery capabilities today is essential to maintaining service delivery during a future crisis, when an adversary may disrupt communications and manipulate control systems.

Links and more information:

CI Fortify | CISA

8. Critical systems security trainings, education

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

!NEW in this feed!:

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

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

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/