BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 October

2026 October, 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 4
4. Book recommendation 9
5. Critical systems security news selection 10
6. Critical systems vulnerabilities 19
7. Critical systems security alerts 32
8. Critical systems security trainings, education 35
9. Critical systems security podcasts 38

1. Critical systems security practices, recommendations

Daily OT Security News

Keeping up with the latest Operational Technology (OT) and ICS cybersecurity developments is essential for maintaining a strong security posture. Because OT environments directly impact physical operations, staying informed about emerging vulnerabilities and threat actor tactics is key to proactive defense.

A great way to build continuous situational awareness is by leveraging dedicated daily OT security blogs and news platforms. While these sources publish updates daily, reviewing them at regular intervals - such as weekly or bi-weekly - is an effective practice. This allows security and technical teams to spot relevant vulnerabilities, track industry trends, and apply actionable threat intelligence to our internal risks without information overload.

Here is a dedicated blog that publishes daily updates on the topic:

Daily OT Security News - Viakoo, Inc



2. Critical systems security conferences

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

OTsec Canada Summit 2026

Canada faces a volatile cyber landscape shaped by rapid AI adoption by adversaries and intensifying state-sponsored threat activity. Nevertheless, Canadian organisations struggle to dedicate necessary resources to OT security, with 81% of organisations experiencing over 25 cybersecurity incidents annually and cyber threats costing the Canadian economy an estimated $9.7 billion.

While new federal frameworks like Bill C-8 set a high bar, many organisations still struggle with complex governance, unmanaged remote vendor access, and persistent legacy system vulnerabilities. In response, OTsec Canada 2026 focuses on "Securing Critical Operations Through Building Practical Cyber Resilience." The meticulously curated programme brings together senior security leaders from Canada's critical sectors to tackle operational technology challenges head-on, exploring proactive strategies that bridge the gap between Bill C-8 policy and practical, ground-level defence.

Montreal, Canada; 3rd – 4th November 2026

More details can be found on the following website:

OTsec Canada | OT Cyber Security Summit | Montréal | November 2026

Industrial Security Conference CPH

Industrial environments are under pressure from every direction. Cyber threats are increasing. Regulations are tightening. IT and OT continue to converge. And critical infrastructure organisations are expected to protect systems that cannot simply be patched, paused, or rebooted.

ISC-CPH exists to help the industry stay ahead of that reality.

For three focused days, security professionals, infrastructure operators, technical specialists, and decision-makers come together to exchange real-world experience, practical insight, and lessons learned from the front lines of industrial security.

From strategic leadership discussions to deep technical workshops, ISC-CPH is built for professionals working with OT, ICS, and critical infrastructure security in practice.

Copenhagen, Denmark; 9th – 11th November 2026

More details can be found on the following website:

Industrial Security Conference Copenhagen – Insight IT

3. Critical systems security incidents

Renfe Cyberattack Hits Spain's Rail Network as AI Role Probed

On September 25, Spain's state-owned railway operator, Renfe, confirmed a cyberattack that compromised customer names and email addresses, though no financial or highly sensitive data was accessed. The attack—believed to be the first AI-driven cyberattack on a Spanish public entity—utilized a system similar to Anthropic's AI and targeted the web infrastructure over several days. Investigators traced the breach back to compromised servers belonging to Adif, the state infrastructure manager, which were interconnected with Renfe's systems.

While Adif's website experienced a temporary outage, train operations and critical services remained fully operational. Renfe noted that the breach followed several weeks of previously blocked intrusion attempts. Upon detection, both organizations isolated affected areas, implemented response protocols, notified the National Cryptologic Center (CCN), and engaged independent experts to contain further risks. Reports indicate the attack was likely orchestrated by a foreign criminal group amid growing international concerns over AI-driven hybrid threats targeting critical infrastructure.

The source is available at the following link:

AI Enters The Renfe Cyberattack Investigation In Spain

4. Book recommendation

OT Security Roadmap

OT Security Roadmap is your complete guide to mastering Operational Technology (OT) and Industrial Cybersecurity. It turns complex security concepts into clear, practical strategies that protect industries, manufacturing plants, and critical infrastructure in today's connected world.

This powerful book helps professionals design, implement, and manage strong OT and ICS cybersecurity programs. It includes frameworks, standards, and real-world examples that ensure digital and physical operations stay secure and reliable.

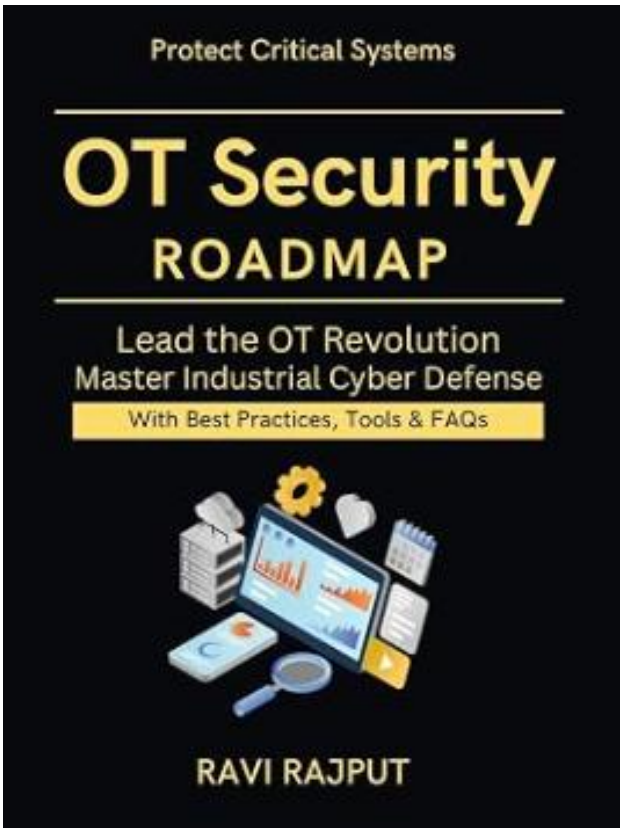
Modern industries rely heavily on interconnected systems that require both safety and stability. This book fulfills the urgent need for industrial cybersecurity by helping readers understand how to secure systems that power manufacturing, utilities, and national infrastructure from advanced cyber threats.

Author/Editor: RAVI RAJPUT (Author)

Year of issue: 2025

The book is available at the following link:

[OT Security Roadmap: Industrial Systems Protection | resilient OT architecture guide | zero trust for OT environments | AI in industrial cybersecurity systems | Global OT security expert handbook eBook : RAJPUT, RAVI: Amazon.in: Kindle Store]



5. Critical systems security news selection

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

1. **Google GTIG finds AI accelerating vulnerability discovery across enterprise and critical infrastructure attack surfaces**
2. **One Packet Can Crash OT Servers in Industrial Sectors**
3. **ClingSTUN Turns Vulnerable IoT Devices Into Proxy Nodes**
4. **Pro-Russia Hacktivists Increase OT Intrusion Claims Across EU**
5. **Is Your OT Team Ready to Lead Through a Cyberattack?**
6. **Anchoring maritime logistics backbone against rising tide of cyber threats targeting ports, vessels, supply chains**
7. **Critical Healthcare Systems Aren't Quantum-Ready**
8. **Even with OT network visibility, critical infrastructure operators struggle with legacy equipment**
9. **Anthropic Fast-Tracks AI Bug Reports to OSS Maintainers, Taps 11 Firms for OT Security**
10. **Rockwell finds 46% of industrial organizations faced cyber incidents as AI adoption, IT/OT convergence reshape resilience**
11. **Hackers Attack French Supermarket Freezers Causing Food Loss**
12. **Anthropic Finds Ingredients for Future AI Worms**
13. **Frontier AI cleared every OT attack goal Booz Allen set in its lab**
14. **AI Takes Control of Robotic Arm in 16 Minutes Flat**
15. **AI Agents Navigate Unfamiliar OT Systems and Move Equipment in Minutes, Booz Allen Finds**
16. **Alms For the Cyber Poor: Program Will Help Small Utilities**
17. **Maritime Coalition Launches Free Vulnerability Database for Ship and Port Systems**
18. **Manufacturing cybersecurity faces persistent governance gaps as accountability, funding, operational priorities diverge**
19. **Long-Hidden Flaws Patched in EPICS Research Facility Control Software**

20. **McCormick introduces Common-Sense Cloud Security Act to strengthen cloud defenses, protect critical infrastructure**
21. **CISA 2030 targets OT modernization, asset visibility, supply chain security through risk-based critical infrastructure defense**

Google GTIG finds AI accelerating vulnerability discovery across enterprise and critical infrastructure attack surfaces

New data from Google Threat Intelligence Group (GTIG) found that artificial intelligence is changing the pace of vulnerability discovery and exploitation, with implications for enterprise and critical infrastructure attack surfaces. Vulnerability disclosures doubled from 5,045 in January 2026 to 10,740 in August, while the average number of vulnerabilities exploited each month increased from 10.5 in 2025 to 18 between January and August 2026. GTIG said the growth in exploitation was driven primarily by rapid weaponization of high-risk, previously disclosed vulnerabilities, rather than a major increase in zero-day exploitation. …

Source and more information:

Google GTIG finds AI accelerating vulnerability discovery across enterprise and critical infrastructure attack surfaces - Industrial Cyber

One Packet Can Crash OT Servers in Industrial Sectors

A now-patched flaw in an open source database used in industrial and Internet of Things (IoT) environments could let unauthenticated attackers crash vulnerable servers with a single specially crafted network packet if not addressed.

The vulnerability, tracked as CVE-2026-42542 affects TDengine, a time-series database that organizations in sectors like manufacturing, energy, automotive, and IoT use to store and analyze large volumes of data collected over time. Examples of such data include readings from sensors and industrial equipment, as well as application- and infrastructure-related performance metrics. …

Source and more information:

One Packet Can Crash OT Servers in Industrial Sectors

ClingSTUN Turns Vulnerable IoT Devices Into Proxy Nodes

Researchers have uncovered a new Linux malware strain that exploits a growing list of known vulnerabilities in Internet of Things (IoT) devices to maintain a persistent foothold on enterprise networks.

What makes the malware especially noteworthy is its use of legitimate public STUN servers to help maintain connectivity with compromised devices, allowing the attackers to obscure their infrastructure in otherwise legitimate Internet traffic. STUN is a protocol that helps devices behind firewalls and NAT connect with each other over the Internet. …

Source and more information:

ClingSTUN Turns Vulnerable IoT Devices Into Proxy Nodes

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

Is Your OT Team Ready to Lead Through a Cyberattack?

When a cyber incident hits an operational technology environment, the stakes can go beyond lost production and downtime to the physical safety of people on the plant floor. Many incident response playbooks remain untested against plant-floor realities.

The question facing manufacturers is no longer whether they have a playbook, but whether their teams can execute it when the alarms go off. …

Source and more information:

Is Your OT Team Ready to Lead Through a Cyberattack?

Anchoring maritime logistics backbone against rising tide of cyber threats targeting ports, vessels, supply chains

Digitization of the marine transportation system has brought deep weaknesses, especially where Terminal Operating Systems (ToS) are involved. A problem at the IT level can stop port operations entirely, freezing logistics and billing even if the physical OT (operational technology) is fine. These systemic weaknesses become more serious because of split accountability. When port authorities, private terminal operators and shipping lines each operate separately there are gaps in how cyber defense's handled. No single entity takes responsibility, which leaves vulnerabilities open. …

Source and more information:

Anchoring maritime logistics backbone against rising tide of cyber threats targeting ports, vessels, supply chains - Industrial Cyber

Critical Healthcare Systems Aren't Quantum-Ready

IT and Internet of Things (IoT) systems across the healthcare sector appear largely unprepared for the post-quantum cryptography (PQC) era, leaving sensitive data potentially vulnerable to "harvest now, decrypt later" attacks.

The situation is particularly acute for Internet-exposed healthcare systems, many of which lack support for TLS 1.3, the foundation for deploying standardized post-quantum cryptography.

Researchers from Forescout Technologies recently analyzed some 2.5 million devices deployed across more than 50 healthcare delivery organizations and uncovered significant gaps in readiness for PQC. …

Source and more information:

Critical Healthcare Systems Aren't Quantum-Ready

Even with OT network visibility, critical infrastructure operators struggle with legacy equipment

Large critical infrastructure operators run seven separate security tools on average, and most still cannot see every asset on their operational technology (OT) networks. That is the picture from a Palo Alto Networks survey of more than 1,600 security and operations leaders.

Old equipment stays on the network

Legacy OT is the most common visibility problem, named by 52 percent of respondents. Another 42 percent call legacy equipment that cannot be patched their biggest cybersecurity risk. Even among respondents who say they see everything, 49 percent still list legacy OT as a challenge. Knowing a machine is there does not update its software. …

Source and more information:

Even with OT network visibility, critical infrastructure operators struggle with legacy equipment - Help Net Security

Anthropic Fast-Tracks AI Bug Reports to OSS Maintainers, Taps 11 Firms for OT Security

Anthropic on Thursday announced two new cybersecurity initiatives: one gives open source maintainers faster access to AI-generated vulnerability reports, and the other targets companies that help secure operational technology (OT).

The programs build on lessons from Project Glasswing. Anthropic said Glasswing partners uncovered many vulnerabilities, but admitted that it has not yet cut cyber risk enough.

According to the company, finding vulnerabilities has never been easier, but verifying, prioritizing and patching them remains hard. Flaws found through Glasswing often took months to get fixed. …

Source and more information:

Anthropic Fast-Tracks AI Bug Reports to OSS Maintainers, Taps 11 Firms for OT Security - SecurityWeek

Rockwell finds 46% of industrial organizations faced cyber incidents as AI adoption, IT/OT convergence reshape resilience

Rockwell Automation disclosed that 46% of industrial organizations experienced a cyber incident in the past year, while 90% said they were confident in their ability to contain a cyber incident. The research also found that 34% of organizations identified cybersecurity as one of the biggest external obstacles to growth over the next 12 months, second only to workforce shortages. At the same time, 62% said they had already invested in cybersecurity platforms such as asset inventory, intrusion detection systems and secure remote access, while cybersecurity ranked as the second-leading return-on-investment driver among technology investments. …

Source and more information:

Rockwell finds 46% of industrial organizations faced cyber incidents as AI adoption, IT/OT convergence reshape resilience - Industrial Cyber

Hackers Attack French Supermarket Freezers Causing Food Loss

Hundreds of French supermarkets have fallen victim to a cyberattack that caused their refrigeration units to heat up, spoiling vast quantities of food and even causing some fires.

Thierry Cotillard, president of the Mousquetaires Group, parent company of the affected Intermarché and Netto chains, told the BFM Business news channel that the experience had been "hell."

"The attack triggered the defrost cycle on all our refrigerated display cases" and raised their temperatures to 50 degree Celsius - 122 degrees Fahrenheit - Cotillard said. "It's a disaster, it's unprecedented, never seen before on this scale." Cotillard said 300 Intermarché and Netto stores had been hit. Industry losses could reach "tens of millions of euros," he said. …

Source and more information:

Hackers Attack French Supermarket Freezers Causing Food Loss

Anthropic Finds Ingredients for Future AI Worms

Self-replicating AI cyberattacks may be on the way, but it doesn't appear to be a practical concern for defenders just yet.

Anthropic's William Zhou and Daniel Freeman published research on Oct. 12 related to commercial IoT devices, AI models' capacity to self-replicate between devices and networks, and whether such replication might be used for malicious computer worms. Zhou and Freeman concluded in the research that "AI models may be months away from being capable enough to self-replicate on commercial internet-of-things (IoT) devices, like smart ovens and off-brand Android TV boxes." ...

Source and more information:

Anthropic Finds Ingredients for Future AI Worms

Frontier AI cleared every OT attack goal Booz Allen set in its lab

Booz Allen set frontier AI models against an isolated industrial-control testbed in its Chantilly, Virginia lab and watched them clear all eight attack objectives it had defined.

The models mapped the network, tied equipment to known weaknesses, wrote working exploits, pivoted into the systems that run production, and in the last test found a robotic arm, took administrative control, and moved it.

The testbed stood in for a manufacturing plant. Hundreds of IT and operational technology devices, real controllers, a SCADA platform, a motor drive, sensors, and that arm, wired into the layered zones a working factory uses. ...

Source and more information:

Frontier AI cleared every OT attack goal Booz Allen set in its lab - Help Net Security

AI Takes Control of Robotic Arm in 16 Minutes Flat

Frontier AI models targeting operational technology (OT) environments, from utilities to factories and beyond, could compromise the network and take control of devices in minutes, according to a fresh round of in-the-lab testing.

Conducted by Booz Allen, the government and military contractor, the tests found that in a typical OT environment, commercial AI models could identify misconfigured devices and work their way through multiple layers of networks to take physical action, the company stated in an October report. In one case, the model was able to take control of and move a robotic arm in an attack that lasted only 16 minutes. ...

Source and more information:

AI Takes Control of Robotic Arm in 16 Minutes Flat

AI Agents Navigate Unfamiliar OT Systems and Move Equipment in Minutes, Booz Allen Finds

A new report from Booz Allen demonstrates that "frontier super intelligence navigated unfamiliar industrial systems, adapted when blocked, and moved physical equipment within minutes."

The findings of the report were presented last week at SecurityWeek's Industrial Control Systems (ICS) Cybersecurity Conference in Nashville, ahead of the public release.

Use of the term 'super intelligence' is, however, confusing. This is not the first time the firm has used it, but it seems to be indistinguishable from the more common term of artificial intelligence (AI). It also quickly follows Donald Trump's September 29, 2026 Executive Order to "replace the term 'Artificial Intelligence' ('AI') with 'Super Intelligence' ('SI') in the executive branch." …

Source and more information:

AI Agents Navigate Unfamiliar OT Systems and Move Equipment in Minutes, Booz Allen Finds - SecurityWeek

Alms For the Cyber Poor: Program Will Help Small Utilities

Dragos, a pioneer in the operational technology security market, and its new backer, consulting giant and global systems integrator Accenture, are teaming up with the Sans Institute training provider and data analytics and search specialist Elastic to offer $10 million worth of free OT cybersecurity support to small and rural utilities.

"We've seen globally that smaller utilities are increasingly the target of cyberattacks with the intent to create physical impact or disrupt operations of [critical service providers like] water and electricity" companies, said Katherine DiEmidio, vice president for public policy and government affairs at Dragos. …

Source and more information:

Alms For the Cyber Poor: Program Will Help Small Utilities

Maritime Coalition Launches Free Vulnerability Database for Ship and Port Systems

Several organizations have teamed up to create Blue Initiative, a public vulnerability database that indexes IT and OT vulnerabilities impacting the maritime industry.

Blue Initiative is the work of cybersecurity company Cydome, Japan's ClassNK classification society, testing and certification giant Bureau Veritas, the Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), and Rakuten Symphony's maritime cybersecurity and digital solutions unit, Rakuten Maritime.

The new project aims to help maritime organizations identify and prioritize vulnerabilities that could threaten their systems. …

Source and more information:

Maritime Coalition Launches Free Vulnerability Database for Ship and Port Systems - SecurityWeek

Manufacturing cybersecurity faces persistent governance gaps as accountability, funding, operational priorities diverge

Security initiatives across manufacturing environments are unlikely to falter due to policy reasons; rather, they are likely to stall due to accountability, financing, and responsibility residing in disparate locations. Across multi-site enterprises, governance standards coexist with uneven delivery. For instance, one plant may be hardened, while another runs unmanaged remote access. Visibility, detection and incident response differ from site to site and in varying proportions across critical infrastructure sectors. …

Source and more information:

Manufacturing cybersecurity faces persistent governance gaps as accountability, funding, operational priorities diverge - Industrial Cyber

Long-Hidden Flaws Patched in EPICS Research Facility Control Software

Four vulnerabilities in EPICS Base could allow attackers to crash processes in control systems used at particle accelerators, fusion experiments and other large research facilities. One flaw could potentially lead to code execution.

CISA disclosed the issues in an advisory published on Tuesday, saying they impact EPICS Base 7.0.10 and earlier. The agency recommends updating to version 7.0.11.

The vulnerabilities were discovered by Cipher, an autonomous security research system made by Causal Security. …

Source and more information:

Long-Hidden Flaws Patched in EPICS Research Facility Control Software - SecurityWeek

McCormick introduces Common-Sense Cloud Security Act to strengthen cloud defenses, protect critical infrastructure

A U.S. Republican Representative from Georgia introduced the Common-Sense Cloud Security Act to strengthen cloud cybersecurity by directing the National Institute of Standards and Technology (NIST) to develop updated standards for protecting sensitive data, preventing cyberattacks and securing critical infrastructure. The legislation would strengthen protections against unauthorized access and malicious activity while establishing a voluntary certification program to help cloud service providers meet modern cybersecurity standards. …

Source and more information:

McCormick introduces Common-Sense Cloud Security Act to strengthen cloud defenses, protect critical infrastructure - Industrial Cyber

CISA 2030 targets OT modernization, asset visibility, supply chain security through risk-based critical infrastructure defense

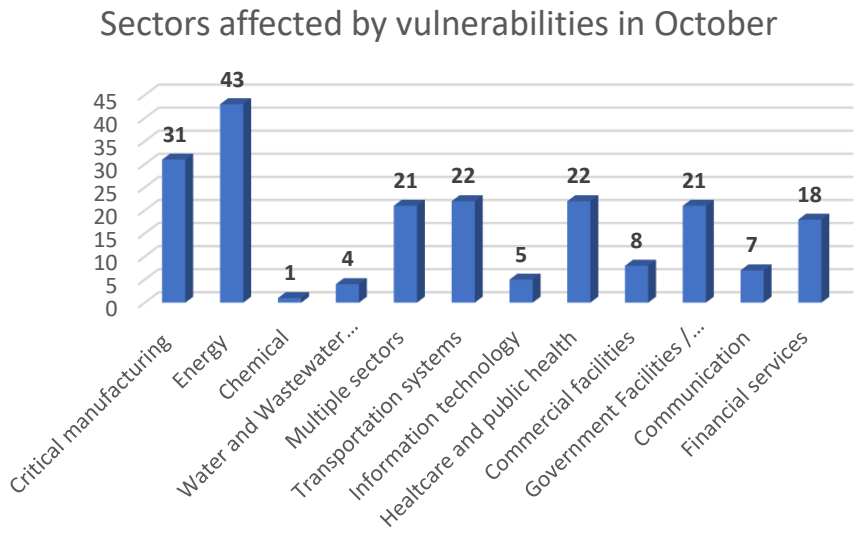
The U.S. Cybersecurity and Infrastructure Security Agency released a new strategy that shifts the nation's cyber defense from passive measures to finding and removing adversaries already inside critical infrastructure networks. Titled 'CISA 2030: Defend, Harden, Prevail,' the document supports the Cyber Strategy for America and the National Resilience Strategy. It calls for concentrating resources on systems whose disruption would most damage national security and the economy. …

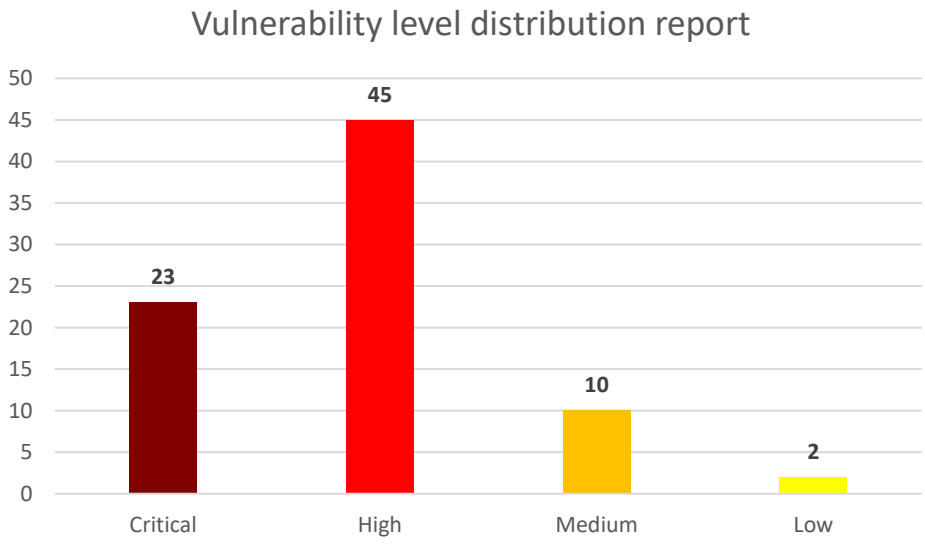
Source and more information:

CISA 2030 targets OT modernization, asset visibility, supply chain security through risk-based critical infrastructure defense - Industrial Cyber

6. Critical systems vulnerabilities

In October 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-26-302-01: **Siemens Mendix SAML Module**

Medium level vulnerability: Authentication Bypass by Capture-replay.

Siemens Mendix SAML Module | CISA

ICSA-26-302-02: **Hitachi Energy TRO600 series products**

High level vulnerabilities: Improper Restriction of Communication Channel to Intended Endpoints, Missing Authentication for Critical Function.

Hitachi Energy TRO600 series products | CISA

ICSA-26-302-03: **Hitachi Energy CoreTec Product**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Write-what-where Condition.

Hitachi Energy CoreTec Product | CISA

ICSA-26-125-01: **Hitachi Energy PCM600 (Update A)**

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

Hitachi Energy PCM600 (Update A) | CISA

ICSA-25-275-02: **Hitachi Energy MSM Product (Update A)**

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

Hitachi Energy MSM Product (Update A) | CISA

ICSA-26-300-01: **EPICS Base**

Critical level vulnerabilities: Integer Overflow or Wraparound, Improper Handling of Length Parameter Inconsistency, Access of Resource Using Incompatible Type ('Type Confusion').

EPICS Base | CISA

ICSA-26-300-02: **Mitsubishi Electric GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32 and BizViz**

Critical level vulnerabilities: Out-of-bounds Write, Weak Password Recovery Mechanism for Forgotten Password, Incorrect Privilege Assignment.

Mitsubishi Electric GENESIS, GENESIS64, ICONICS Suite, Hyper Historian, AnalytiX, MobileHMI, IoTWorX, MC Works64, GENESIS32 and BizViz | CISA

ICSA-26-267-02: **Eufy Omni C20, Omni X10 Pro (Update A)**

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 (Update A) | CISA

ICSMA-26-295-01: **InterSystems Corporation InterSystems IRIS for Health**

High level vulnerability: Cleartext Transmission of Sensitive Information.

InterSystems Corporation InterSystems IRIS for Health | CISA

ICSA-26-295-01: **Kiloview E3 NDI Encoder**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Missing Authentication for Critical Function, Insufficient Session Expiration, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), NULL Pointer Dereference, Use of Hard-coded Credentials.

Kiloview E3 NDI Encoder | CISA

ICSA-26-295-02: **Siemens Industrial Edge App Publisher**

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

Siemens Industrial Edge App Publisher | CISA

ICSA-26-295-03: **Siemens Software Center**

Medium level vulnerability: Uncontrolled Search Path Element.

Siemens Software Center | CISA

ICSA-26-295-04: **Siemens Capital Embedded AR Classic**

Medium level vulnerability: Out-of-bounds Read.

Siemens Capital Embedded AR Classic | CISA

ICSA-26-295-05: **Siemens SENTRON 3NA COM Fuse**

Medium level vulnerability: Improper Verification of Source of a Communication Channel.

Siemens SENTRON 3NA COM Fuse | CISA

ICSA-26-295-06: **Siemens PSS(R)SINCAL**

High level vulnerability: Out-of-bounds Write.

Siemens PSS(R)SINCAL | CISA

ICSA-26-295-07: **Siemens SIMATIC IPCs**

High level vulnerability: Use of Default Cryptographic Key.

Siemens SIMATIC IPCs | CISA

ICSA-26-295-08: **Siemens APOGEE, TALON and Desigo PXC/PXM Products**

High level vulnerabilities: Out-of-bounds Read, Integer Underflow (Wrap or Wraparound), Stack-based Buffer Overflow.

Siemens APOGEE, TALON and Desigo PXC/PXM Products | CISA

ICSA-26-295-09: **Siemens Industrial Edge Device Kit**

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

Siemens Industrial Edge Device Kit | CISA

ICSA-26-295-10: **Siemens SIMATIC S7 Webserver API**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Generation of Error Message Containing Sensitive Information.

Siemens SIMATIC S7 Webserver API | CISA

ICSA-26-295-11: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP**

Critical level vulnerabilities: Access of Resource Using Incompatible Type ('Type Confusion'), Access of Uninitialized Pointer, Active Debug Code, Buffer Access with Incorrect Length Value, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Buffer Underwrite ('Buffer Underflow'), Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Deadlock, Divide By Zero, Expired Pointer Dereference, Exposure of Sensitive Information Due to Incompatible Policies, Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution, Improper Enforcement of Behavioral Workflow, Improper Following of Specification by Caller, Improper Handling of Invalid Use of Special Elements, Improper Handling of Length Parameter Inconsistency, Improper Handling of Missing Special Element, Improper Handling of Structural Elements, Improper Input Validation, Improper Locking, Improper Neutralization of Null Byte or NUL Character, Improper Null Termination, Improper Privilege Management, Improper Resource Locking, Improper Resource Shutdown or Release, Improper Update of Reference Count, Improper Validation of Specified Index, Position, or Offset in Input, Improper Validation of Specified Quantity in Input, Improper Validation of Specified Type of Input, Improperly Implemented Security Check for Standard, Incomplete Cleanup, Incomplete Internal State Distinction, Incorrect Calculation of Buffer Size, Incorrect Conversion between Numeric Types, Incorrect Privilege Assignment, Incorrect Synchronization, Incorrect Type Conversion or Cast, Integer Overflow or Wraparound, Loop with Unreachable Exit Condition ('Infinite Loop'), Memory Allocation with Excessive Size Value, Misinterpretation of Input, Missing Critical Step in Authentication, Missing Default Case in Multiple Condition Expression, Missing Encryption of Sensitive Data, Missing Initialization of Resource, Missing Release of Memory after Effective Lifetime, Missing Release of Resource after Effective Lifetime, Missing Report of Error Condition, Missing Synchronization, Multiple Releases of Same Resource or Handle, NULL Pointer Dereference, Operation on a Resource after Expiration or Release, Out-of-bounds Read, Out-of-bounds Write, Plaintext Storage of a Password, Race Condition within a Thread, Reachable Assertion, Release of Invalid Pointer or Reference, Signal Handler Race Condition, Time-of-check Time-of-use (TOCTOU) Race Condition, Transmission of Private Resources into a New Sphere ('Resource Leak'), Trust of System Event Data, Unchecked Return Value, Uncontrolled Recursion, Untrusted Pointer Dereference, Use After Free, Use of Externally-

Controlled Format String, Use of Uninitialized Resource, Use of Uninitialized Variable, Write-what-where Condition.

Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP | CISA

ICSA-26-295-12: **Siemens RUGGEDCOM CROSSBOW**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Authorization Bypass Through User-Controlled Key, Insertion of Sensitive Information Into Sent Data, Client-Side Enforcement of Server-Side Security.

Siemens RUGGEDCOM CROSSBOW | CISA

ICSA-26-295-13: **Siemens WinCC**

High level vulnerability: Incorrect Privilege Assignment.

Siemens WinCC | CISA

ICSA-26-295-14: **Siemens SIMATIC S7 PLCs Web Server**

Critical level vulnerabilities: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Siemens SIMATIC S7 PLCs Web Server | CISA

ICSA-26-295-15: **Siemens RUGGEDCOM CROSSBOW Station Access Controller**

Critical level vulnerabilities: Numeric Truncation Error, Improper Clearing of Heap Memory Before Release ('Heap Inspection'), Improper Handling of Unicode Encoding, Heap-based Buffer Overflow.

Siemens RUGGEDCOM CROSSBOW Station Access Controller | CISA

ICSA-26-295-16: **Siemens SIMATIC S7-1500 TM MFP**

Critical level vulnerabilities: Access of Uninitialized Pointer, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Deadlock, Detection of Error Condition Without Action, Double Free, Expired Pointer Dereference, Heap-based Buffer Overflow, Improper Control of Resource Identifiers ('Resource Injection'), Improper Control of a Resource Through its Lifetime, Improper Handling of Length Parameter Inconsistency, Improper Handling of Missing Special Element, Improper Handling of Structural Elements, Improper Input Validation, Improper Locking, Improper Resource Locking, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Update of Reference Count, Improper Validation of Array Index, Improper Validation of Consistency within Input, Improper Validation of Specified Index, Position, or Offset in Input, Improper Validation of Specified Quantity in Input, Improper Validation of Specified Type of Input, Incorrect Synchronization, Integer Overflow or Wraparound, Integer Underflow (Wrap or Wraparound), Loop with Unreachable Exit Condition ('Infinite Loop'), Missing Default Case in Multiple Condition Expression, Missing Initialization of Resource, Missing Lock Check, Missing Release of Memory after Effective Lifetime, Missing Release of Resource after Effective Lifetime, Multiple Locks of

a Critical Resource, NULL Pointer Dereference, Operation on a Resource after Expiration or Release, Out-of-bounds Read, Out-of-bounds Write, Plaintext Storage of a Password, Release of Invalid Pointer or Reference, Return of Wrong Status Code, Signal Handler Race Condition, Time-of-check Time-of-use (TOCTOU) Race Condition, Unchecked Return Value, Use After Free, Use of Incorrect Operator, Use of Uninitialized Resource, Write-what-where Condition.

Siemens SIMATIC S7-1500 TM MFP | CISA

ICSA-26-295-17: **Siemens Industrial Edge Devices**

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

Siemens Industrial Edge Devices | CISA

ICSA-26-295-18: **Siemens RUGGEDCOM APE1808 Devices**

High level vulnerabilities: Improper Neutralization of Special Elements Used in a Template Engine, Incorrect Authorization, Lack of Administrator Control over Security, Cross-Site Request Forgery (CSRF).

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-26-274-06: **Meari IoT Cloud Platform OpenAPI Service (Update A)**

High level vulnerability: Missing Authorization.

Meari IoT Cloud Platform OpenAPI Service (Update A) | CISA

ICSA-26-293-01: **HMS Networks PEAK-System PCAN Windows drivers**

High level vulnerabilities: Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Validation of Array Index, Untrusted Pointer Dereference, Improper Handling of Length Parameter Inconsistency.

HMS Networks PEAK-System PCAN Windows drivers | CISA

ICSA-26-293-03: **Moxa AIG-302 ThingsPro Edge**

High level vulnerabilities: Missing Authorization, Use of Hard-coded Cryptographic Key.

Moxa AIG-302 ThingsPro Edge | CISA

ICSA-26-293-04: **Hitachi Energy MicroSCADA X SYS600 Product**

High level vulnerabilities: Improper Neutralization of Formula Elements in a CSV File, Incorrect Implementation of Authentication Algorithm.

Hitachi Energy MicroSCADA X SYS600 Product | CISA

ICSA-26-293-05: **Hitachi Energy RTU500 Product**

High level vulnerabilities: NULL Pointer Dereference, Access of Resource Using Incompatible Type ('Type Confusion'), Use After Free, Cleartext Transmission of Sensitive Information, Insufficiently Protected Credentials, Authentication Bypass by Capture-replay, Authentication Bypass by Primary Weakness.

Hitachi Energy RTU500 Product | CISA

SSA-580366: **DLL Sideloading Vulnerability in Siemens Software Center (Update: 1.2.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-580366

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: 1.2.)**

High level vulnerabilities: Multiple.

SSA-019113

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: 1.7.)**

High level vulnerabilities: Multiple.

SSA-082556

SSA-104023: **Multiple Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices (Update: 1.2.)**

Critical level vulnerabilities: Multiple.

SSA-104023

SSA-127084: **Multiple Vulnerabilities in Fortigate NGFW before V7.6.7 on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Stack-based Buffer Overflow, Allocation of Resources Without Limits or Throttling, Improper Validation of Certificate with Host Mismatch.

SSA-127084

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1 (Update: 2.3.)**

High level vulnerabilities: Multiple.

SSA-265688

SSA-267056: **Multiple Vulnerabilities in LOGO! 8 BM Devices (Update: 1.1.)**

High level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Missing Authentication for Critical Function.

SSA-267056

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 2.0.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-392859: **Local Arbitrary Code Execution Vulnerability in Siemens Engineering Platforms before V20 (Update: 1.4.)**

High level vulnerability: Improper Input Validation.

SSA-392859

SSA-398330: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP >= V3.1.0 and < V3.1.5 (Update: 2.8.)**

High level vulnerabilities: Multiple.

SSA-398330

SSA-434797: **Buffer Overflow Vulnerability in OpenSSL affecting Siemens Products (Update: 1.4.)**

High level vulnerability: Out-of-bounds Write.

SSA-434797

SSA-493396: **Deserialization Vulnerability in Siemens Engineering Platforms (Update: 1.3.)** **High** level vulnerability: Deserialization of Untrusted Data.

SSA-493396

SSA-545643: **Multiple Vulnerabilities in KACO Blueplanet Inverters (Update: 1.2.)**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

SSA-545643

SSA-563922: **Local Privilege Escalation Vulnerability in SIMOTION Tools (Update: 1.1.)**

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

SSA-563922

SSA-628843: **Out of Bound Read Vulnerability in TPM 2.0 (Update: 1.2.)**

Medium level vulnerability: Out-of-bounds Read.

SSA-628843

SSA-693808: **Deserialization Vulnerability in Siemens Engineering Platforms (Update: 1.4.)** **High** level vulnerability: Deserialization of Untrusted Data.

SSA-693808

SSA-794185: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SIPROTEC, SICAM and Related Products (Update: 1.4.)**

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

SSA-794185

SSA-794697: **Vulnerabilities in the Additional GNU/Linux Subsystem of the SIMATIC S7-1500 TM MFP Before V1.1 (Update: 1.9.)**

Critical level vulnerabilities: Multiple.

SSA-794697

SSA-800126: **Deserialization Vulnerability in Siemens Engineering Platforms before V20 (Update: 1.3.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-800126

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

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

SSA-858251

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW before V7.6.6 on RUGGEDCOM APE1808 Devices (Update: 2.1.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-967325: **Multiple Vulnerabilities in Palo Alto Networks PAN-OS before V11.2.10-h7 on RUGGEDCOM APE1808 Devices (Update: 1.3.)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Reliance on Cookies without Validation and Integrity Checking, Server-Side Request Forgery (SSRF), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Check for Unusual or Exceptional Conditions, Heap-based Buffer Overflow, Improper Verification of Cryptographic Signature, Out-of-bounds Write, Use of Uninitialized Resource.

SSA-967325

ICSA-26-280-01: **CISA Malcolm**

High level vulnerabilities: Authentication Bypass by Spoofing, Incorrect Authorization, Server-Side Request Forgery (SSRF), Authentication Bypass Using an Alternate Path or Channel, Cross-Site Request Forgery (CSRF), Improper Handling of Highly Compressed Data (Data Amplification).

CISA Malcolm | CISA

ICSA-26-288-01: **Eclipse Foundation Eclipse Milo**

High level vulnerabilities: Incorrect Authorization, Missing Release of Memory after Effective Lifetime, Missing Authorization, Observable Response Discrepancy, Missing Release of Resource after Effective Lifetime.

Eclipse Foundation Eclipse Milo | CISA

ICSA-26-288-02: **Guangzhou Juan IoT Technology EseeCloud**

Critical level vulnerabilities: Use of Hard-coded Credentials, Improperly Controlled Modification of Dynamically-Determined Object Attributes, Observable Response Discrepancy.

Guangzhou Juan IoT Technology EseeCloud | CISA

ICSMA-26-288-01: **Thermo Fisher Torrent Suite**

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

Thermo Fisher Torrent Suite Software | CISA

ICSMA-26-288-02: **J4Care dcm4che**

Critical level vulnerabilities: Missing Authorization, Loop with Unreachable Exit Condition ('Infinite Loop'), Inefficient Algorithmic Complexity, Missing Authentication for Critical Function.

J4Care dcm4che | CISA

ICSA-26-281-01: **Red Lion Controls N-Tron 700 Series (Update A)**

High level vulnerabilities: Use of Hard-coded Credentials, Insufficiently Protected Credentials, Storing Passwords in a Recoverable Format, Missing Authentication for Critical Function, Download of Code Without Integrity Check, Reachable Assertion, Authentication Bypass Using an Alternate Path or Channel.

Red Lion Controls N-Tron 700 Series (Update A) | CISA

ICSA-26-286-01: **Inductive Automation Ignition Software**

High level vulnerability: Incorrect Authorization.

Inductive Automation Ignition Software | CISA

ICSA-26-286-02: **Swann Communications SWIFI-SE2KIC**

Medium level vulnerability: Missing Authentication for Critical Function.

Swann Communications SWIFI-SE2KIC | CISA

ICSA-26-281-01: **Red Lion Controls N-Tron 700 Series**

High level vulnerabilities: Use of Hard-coded Credentials, Insufficiently Protected Credentials, Storing Passwords in a Recoverable Format, Missing Authentication for Critical Function, Download of Code Without Integrity Check, Reachable Assertion, Authentication Bypass Using an Alternate Path or Channel.

Red Lion Controls N-Tron 700 Series | CISA

ICSA-26-281-02: **Grid Protection Alliance openPDC and openHistorian**

Critical level vulnerabilities: Deserialization of Untrusted Data, Missing Authentication for Critical Function, Server-Side Request Forgery (SSRF), Use of Hard-coded Credentials, Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection').

Grid Protection Alliance openPDC and openHistorian | CISA

ICSA-26-281-03: **Satel Netco Design**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Inefficient Regular Expression Complexity, Relative Path Traversal.

Satel Netco Design | CISA

ICSA-26-069-02: **Lantronix EDS3000PS and EDS5000 (Update B)**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Authentication Bypass Using an Alternate Path or Channel, Unverified Password Change.

Lantronix EDS3000PS and EDS5000 (Update B) | CISA

ICSMA-26-223-02: **Pulsetto Vagus Nerve Stimulator (Update A)**

High level vulnerability: Hidden Functionality.

Pulsetto Vagus Nerve Stimulator (Update A) | CISA

ICSA-25-259-02: **Hitachi Energy RTU500 series (Update A)**

High level vulnerabilities: NULL Pointer Dereference, Improper Validation of Integrity Check Value, Integer Overflow or Wraparound, Heap-based Buffer Overflow, Improper Restriction of XML External Entity Reference, Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'), Stack-based Buffer Overflow.

Hitachi Energy RTU500 Series (Update A) | CISA

ICSA-26-279-01: **Johnson Control EasyIO FG**

High level vulnerabilities: Use of Hard-coded Credentials, Improper Privilege Management.

Johnson Controls EasyIO FG | CISA

ICSA-26-279-02: **Savannah lwIP**

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

Savannah lwIP SMTP client | CISA

ICSA-26-279-03: **Hitachi Energy Asset Suite**

High level vulnerability: Missing Authentication for Critical Function.

Hitachi Energy Asset Suite | CISA

ICSA-26-279-04: **Hitachi Energy SOI**

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

Hitachi Energy SOI | CISA

ICSA-26-279-05: **Hitachi Energy REB500**

Medium level vulnerabilities: Uncontrolled Recursion, Allocation of Resources Without Limits or Throttling.

Hitachi Energy REB500 | CISA

ICSA-26-279-06: **Hitachi Energy RTU500 series CMU Firmware**

Critical level vulnerabilities: Missing Authentication for Critical Function, Relative Path Traversal, Missing Authorization, Incorrect Authorization, Download of Code Without Integrity Check.

Hitachi Energy RTU500 | CISA

ICSA-26-274-01: **Armatura LLC Armatura One**

Critical level vulnerabilities: Deserialization of Untrusted Data, Use of Hard-coded Cryptographic Key, Use of Hard-coded Credentials, Insertion of Sensitive Information into Log File.

Armatura LLC Armatura One | CISA

ICSA-26-274-02: **Monta monta.app**

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

Monta monta.app | CISA

ICSA-26-274-03: **ABB Protection and Control IED Manager PCM600**

Medium level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

ABB Protection and Control IED Manager PCM600 | CISA

ICSA-26-274-04: **Johnson Controls EasyIO Neo Series EC and CW Controllers**

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

Johnson Controls EasyIO Neo Series EC and CW Controllers | CISA

ICSA-26-274-05: **Johnson Controls EasyIO Neo Series EC and CW Controllers**

Medium level vulnerability: Cleartext Transmission of Sensitive Information.

Johnson Controls EasyIO Neo Series EC and CW Controllers | CISA

ICSA-26-274-06: **Meari IoT Cloud Platform OpenAPI Service**

High level vulnerability: Missing Authorization.

Meari IoT Cloud Platform OpenAPI Service | 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 October:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-104286 Fortinet FortiMail Path Traversal Vulnerability;
CVE-2026-102489 Zammad GmbH Zammad Session Fixation Vulnerability;
CVE-2026-102490 Zammad GmbH Zammad Improper Privilege Management Vulnerability;
CVE-2026-88779 Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability;
CVE-2026-96951 Microsoft Windows Command Injection Vulnerability;
CVE-2026-104935 Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability;
CVE-2026-0322 Palo Alto Networks PAN-OS Code Injection Vulnerability;
CVE-2026-76519 Cisco Secure Email Gateway Relative Path Traversal Vulnerability;
CVE-2026-105133 Ahsay AhsayCBS Improper Authentication Vulnerability;
CVE-2026-105134 Ahsay AhsayCBS Command Injection Vulnerability;
CVE-2026-21589 Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability;
CVE-2025-61624 Fortinet Multiple Products Path Traversal Vulnerability;
CVE-2026-102764 BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability;
CVE-2026-96652 Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2026-96654 Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability;
CVE-2026-96655 Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2026-96656 Plex Media Server External Control of File Name or Path Vulnerability;
CVE-2026-106931 EG Secure Solutions SiteGuard Server Edition OS Command Injection Vulnerability;
CVE-2026-110936 Siemens Software Center Uncontrolled Search Path Element Vulnerability;
CVE-2026-114625 Arista VeloCloud Orchestrator SQL Injection Vulnerability;
CVE-2026-110447 Collabora Online – Built-in CODE Server OS Command Injection Vulnerability;
CVE-2026-109618 – PHP Memory Corruption Vulnerability;
CVE-2026-109619 – PHP Stale Internal Request-State Vulnerability;
CVE-2026-48356 Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability;
CVE-2026-111497 Google Brotli Unchecked Return Value Vulnerability;
CVE-2026-41709 Broadcom VMWare ESX Insufficient Logging Vulnerability;
CVE-2026-46300 Linux Kernel Missing Initialization of a Variable Vulnerability;

CVE-2026-97229 GitLab Community Edition and Enterprise Edition Integer Overflow or Wraparound vulnerability;
CVE-2026-76418 Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability;
Links and more information:
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
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four 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 Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two 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 Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure
CISA is aware of Ivanti's disclosure of a newly exploited vulnerability, CVE-2026-104935, affecting Ivanti Connect Secure versions 25.1.1.1 and prior, 25.1.2.2 and prior, and 22.8R2.4 and prior. CISA is aware of cyber threat actors exploiting this zero-day authentication bypass vulnerability, which allows remote, unauthenticated execution of arbitrary commands, to conduct credential theft and data exfiltration. CISA added CVE-2026-104935 to its Known Exploited Vulnerabilities (KEV) Catalog on Oct. 13, 2026.
Source and more information:
CISA Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure | CISA

CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support
CISA is aware of critical authentication bypass vulnerability CVE-2026-102764, affecting BeyondTrust Remote Support (formerly Bomgar) versions 26.2.3 and earlier. Patches are available for supported versions (24.3.1 and later); organizations using older versions must upgrade first. Cyber threat actors are actively exploiting the vulnerability to gain initial access, then establishing persistence, escalating privileges, and moving laterally. CISA added CVE-2026-102764 to its Known Exploited Vulnerabilities (KEV) catalog on Oct. 16, 2026.
Source and more information:
CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support | CISA

Critical Vulnerabilities in PHP Require Immediate Patching

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog and updated the PHP Alert, Critical Vulnerabilities in PHP Require Immediate Patching.

- *CVE-2026-109618 – PHP Memory Corruption Vulnerability*
- *CVE-2026-109619 – PHP Stale Internal Request-State Vulnerability*

These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risks to the federal enterprise.

Source and more information:

Critical Vulnerabilities in PHP Require Immediate Patching | CISA

8. Critical systems security trainings, education

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