BLACK CELL
Protecting critical infrastructures

Industrial Control Systems security feed

2026 March

2026 March, Industrial Control Systems security feed

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

List of Contents

1. ICS good practices, recommendations

ICS security best practices: How to protect Industrial Control Systems

Industrial Control Systems (ICS) form the backbone of modern manufacturing, utilities, and critical infrastructure, yet they are increasingly targeted by cyber attackers due to their operational importance and traditionally weak security posture. As ICS and Operational Technology (OT) environments become more connected to IT networks, organizations must implement robust cybersecurity measures to protect against sophisticated threats.

Key Best Practices for ICS Cybersecurity

1. Network Segmentation and Secure Architecture

Segment ICS/OT networks into isolated zones to limit access and reduce the blast radius of a potential compromise. Firewalls, VLANs, demilitarized zones (DMZs), and strict access policies help enforce boundaries between IT and ICS domains and control lateral movement.

2. Strong Authentication and Access Control

Implement multi-factor authentication (MFA) and role-based access control (RBAC) for all ICS interfaces. Enforcing unique user identities, strong passwords, and periodic credential rotation mitigates risks from compromised credentials and unauthorized access.

3. Regular Patching and Updates

Keep ICS software, firmware, and control applications up to date. Legacy systems are common attack vectors, so a risk-aware patching strategy - combined with testing in staging environments - helps reduce vulnerability exposure without disrupting uptime.

4. Secure Remote Access

Operators and vendors often require remote access to ICS devices. Safeguard these connections using encrypted VPNs and strictly controlled access policies to prevent credential theft and unauthorized access via insecure networks.

5. Employee Awareness and Training

Human error remains a significant threat vector. Regular training on phishing recognition, secure credential handling, and ICS-specific procedures builds a culture of security awareness that complements technical controls.

6. Threat Intelligence and Monitoring

Leverage up-to-date threat intelligence to understand active adversary tactics and emerging vulnerabilities. Real-time monitoring can help detect anomalous behavior and provide early warning of potential incidents.

Implementing these practices help strengthen the resilience of ICS environments, protect critical operational processes, and reduce the likelihood of costly disruptions due to cyber incidents.

For more in-depth guidance and tailored support on securing industrial systems, consider industry frameworks such as ISA/IEC 62443 and integrate these best practices into your organizational risk management strategy.

Source and links and more information:

https://nordlayer.com/blog/ics-security-best-practices/

2. ICS conferences

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

CS4CA APAC

With the APAC increasingly taking a proactive stance on the protection of its systems from cyber attacks, the threat to the region's organisations and critical infrastructure has never been clearer. From geopolitical shifts to supply chain risk, the cyberattack surface has expanded—raising both the likelihood and consequence of disruption to the organisations that keep the APAC economy running.

Discussing these issues and more, the APAC edition of the globally acclaimed CS4CA (Cyber Security for Critical Assets) Series of OT cyber security summits will return to Singapore on 1-2 April 2026 for its 7th edition. The Summit will be co-hosted with our APAC Cyber Summit, an IT security event for all industries, returning for the 3rd year. Under the theme of Industrial Fortification: Building an Integrated & Resilient OT Ecosystem for CS4CA and Integrated Defence: APAC IT Security in the Age of Global Risk for the Cyber Summit, we are bringing together 150+ like-minded, senior IT and OT security stakeholders from APAC's biggest and most important industries.

Singapore, Singapore; 1st – 2nd April 2026

More details can be found on the following website:

https://apac.cs4ca.com/

OT.SEC.CON. 2026

Join Industrial Defender at OT.SEC.CON. 2026. OT.SEC.CON. Is the Houston-area OT security conference where operational technology meets cybersecurity in a groundbreaking event designed to bridge the gap between owner/operators and cybersecurity experts. Learn insights and strategies about OT security and get a demo from the team with your specific OT environment in mind.

Houston, TX, USA; 1st – 2nd April 2026

More details can be found on the following website:

https://www.industrialdefender.com/events/ot-sec-con-2026

Level Zer0

Join the premier event for Industrial Control System and Operational Technology (ICS/OT) cyber security professionals, where engineering meets cyber security to protect critical infrastructure.

The Level Zero Conference brings experts from across industries together to address the complex challenges of securing operational technology. The multidisciplinary approach integrates engineering, cyber security, and risk management to safeguard critical infrastructure from level zero to the cloud.

Atlanta, GA, USA; 20th – 22nd April 2026

More details can be found on the following website:

https://levelzeroconference.com/

ICS Lockdown

As an online extension of SecurityWeek's ICS Cybersecurity Conference – the original ICS/SCADA cyber security event that has been running since 2002 – ICS Lockdown 2026 is virtual conference that will dive deep into the world of industrial cybersecurity and help those charged with protecting operational technology (OT) environments defend against cyber threats.

Virtual; 29th April 2026

More details can be found on the following website:

https://www.securitysummits.com/event/ics-lockdown/

3. ICS incidents

Web Server Exploits and Mimikatz Used in Attacks Targeting Asian Critical Infrastructure

A long-running cyber espionage campaign has targeted high-value organizations across South, Southeast, and East Asia, affecting sectors that play a crucial role in national and regional critical infrastructure. According to research by Palo Alto Networks Unit 42, the activity has been attributed to a previously undocumented threat cluster referred to as CL-UNK-1068. While the group's exact affiliation remains unclear, analysts assess with moderate-to-high confidence that the campaign is primarily focused on cyber espionage.

The attackers have targeted organizations in aviation, energy, telecommunications, government, law enforcement, pharmaceuticals, and technology. Many of these industries form part of essential infrastructure ecosystems, where cyber intrusions can have significant strategic and operational implications. Such environments often combine conventional IT systems with operational technology (OT) components, increasing the potential impact of unauthorized access or data exfiltration.

The threat actors rely on a versatile toolset that combines custom malware, modified open-source utilities, and legitimate system tools, allowing them to maintain persistence while remaining difficult to detect. Among the tools identified were widely known web shells such as Godzilla and ANTSWORD, the Linux backdoor Xnote, and Fast Reverse Proxy (FRP) for maintaining covert remote access. These tools allow attackers to operate across both Windows and Linux environments, which is typical in large enterprise and infrastructure networks.

Initial access in many cases appears to involve the exploitation of vulnerable web servers, after which attackers deploy web shells to execute commands remotely. From there, they attempt to move laterally within the environment, searching for sensitive files and configuration data. Targeted information includes web application files, browser histories, spreadsheets, and database backups. In critical infrastructure environments, such data may reveal system configurations, access credentials, or internal network structures that could support further espionage or future attacks.

One particularly unusual technique observed in the campaign involves a stealthy data exfiltration method designed to bypass security monitoring. Instead of directly transferring files from compromised systems, the attackers archive the data, encode it as Base64 text using built-in system tools, and display the encoded output through the web shell interface. This allows them to retrieve the information without initiating traditional file transfers, reducing the likelihood of detection.

Credential theft also plays a key role in the campaign. The attackers deploy a range of tools to extract passwords and authentication data from memory and configuration files, enabling them to expand their access across the compromised network.

The campaign highlights a growing risk for critical infrastructure operators, where attackers increasingly target supporting IT environments as an entry point for intelligence gathering. Even when industrial control systems are not directly affected, compromised IT systems can expose sensitive operational data or provide a pathway toward more critical network

segments. The incident underscores the importance of network segmentation, strong credential protection, and continuous monitoring in environments that support essential services and industrial operations.

The source is available at the following link:

https://thehackernews.com/2026/03/web-server-exploits-and-mimikatz-used.html

4. Book recommendation

Implementing IEC 62443 - A Pragmatic Approach to Cybersecurity

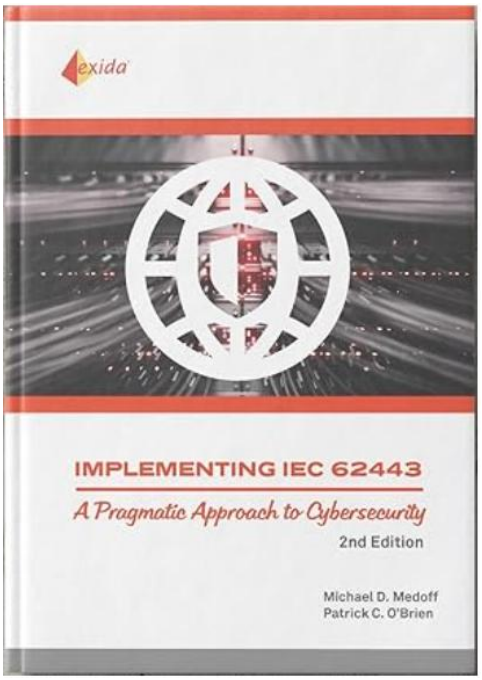
How is the cybersecurity landscape for automation systems changing? How does the IEC 62443 cybersecurity standard apply to today s automation systems? How can I improve cybersecurity for my organization without making my system inoperable? You can find the answers to these questions and more in Implementing IEC 62443, A Pragmatic Approach to Cybersecurity. The concepts and techniques presented in this book are based on the application of the cybersecurity lifecycle as it is described in the international standard IEC 62443. These concepts can be readily applied in cybersecurity applications across all industry sectors. The book expands upon the framework developed in the standards to provide a practical guide for applying these concepts and techniques to both new and existing plants. The techniques cover a range from qualitative screening to a semi quantitative method for SL verification and provides guidance across the entire cybersecurity lifecycle.

Author/Editor: Michael D. Medoff (Author), Patrick C. O'Brien (Author)

Year of issue: 2022

The book is available at the following link:

Implementing IEC 62443 - A Pragmatic Approach to Cybersecurity | exida



5. ICS security news selection

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

1. **'Richter Scale' Model Measures Magnitude of OT Cyber Incidents**
2. **Overcoming Security Challenges in Remote Energy Operations**
3. **US-Israeli campaign triggers Iranian counteroffensive targeting Gulf energy, critical infrastructure**
4. **AI-assisted credential attacks on FortiGate devices could expose OT networks to ransomware staging**
5. **Quantum-Resistant Data Diode Secures Sensitive Data on Edge Devices, Critical Systems**
6. **As War Continues, Pro-Iranian Actors Launch Barrage of Cyberattacks**
7. **The Decoupling Phase and the Capital Reckoning Behind OT Convergence**
8. **The Availability Imperative (Why OT Security Demands Protocol-Specific Firewalls)**
9. **5 Best Practices For Managing Remote Access To Industrial Equipment**
10. **NIST Urged to Go Deep in OT Security Guidance**
11. **Webinar Today: Designing an OT SOC for Safety, Reliability, and Business Continuity**
12. **Kai Emerges From Stealth With $125M in Funding for AI Platform Bridging IT and OT Security**
13. **Stop fixing OT security with IT thinking**
14. **Data Diodes Have Become Essential to Modern OT Cybersecurity**
15. **Building 'Incident Management for Industrial Control Systems' to address gaps in OT cyber incident response**
16. **Poland's nuclear research centre targeted by cyberattack**
17. **New York introduces cybersecurity rules, $2.5 million grant program to strengthen water infrastructure defenses**
18. **Beyond CVSS: OT Security Looks for Its Risk Methodology**
19. **Claroty reports 82% of CPS attacks used remote access protocols as hacktivists target HMIs and SCADA at scale**

20. **Mitsubishi Deal Gives Nozomi Broader OT Security Reach**
21. **DOE Sets 5-Year Plan to Harden US Grid Against Cyberattacks**
22. **Crisis lessons from OT incident response as cyber-physical attacks unfold within normal industrial operations**
23. **How Cyberattacks Can Turn Battery Farms Into Grid Blackouts**
24. **Rising ICS incidents drive shift from reactive risk models to intelligence-driven OT security strategies**
25. **Lesson From Enigma Cipher Machine Shapes OT Sec Strategy**

'Richter Scale' Model Measures Magnitude of OT Cyber Incidents

S4x26, MIAMI — Feb. 24, 2026 — A newly developed method for gauging the impact of an OT cybersecurity incident could pave the way for more accurate measurement and response to an event, and also shine light on risk and business ramifications.

The Operational Technology Incident (OTI) Impact Score — which will be unveiled today at the ICS/OT industry's S4x26 Conference in Miami — aims to provide rapid clarity on the actual effects of OT cyber incidents, which often get over- or under-hyped, according to Dale Peterson, co-creator of the OTI model and head of ICS/OT consulting and research firm Digital Bond. …

Source and more information:

https://www.darkreading.com/ics-ot-security/richter-scale-model-measures-cyber-incidents

Overcoming Security Challenges in Remote Energy Operations

Renewable energy companies are facing growing threats from cybercriminals as they expand their operations. Wind turbine farms located offshore and other remote facilities are especially vulnerable because they are hard to reach and secure.

The security landscape for remote facilities has shifted "dramatically," and energy providers can no longer rely on isolation for protection, said Nir Ayalon, founder and CEO of Cydome, a maritime and critical infrastructure cybersecurity firm.

"These sites are just as exposed as a corporate office - but with far more complex operational challenges," Ayalon said. …

Source and more information:

https://www.ot.today/overcoming-security-challenges-in-remote-energy-operations-a-30741

US-Israeli campaign triggers Iranian counteroffensive targeting Gulf energy, critical infrastructure

Iran has entered its third consecutive day of near-total internet blackout as the coordinated U.S.-Israeli cyber and military campaign has pushed the confrontation into what analysts describe as an unprecedented digital battlefield. At the same time, pro-Iran hacking groups are signaling retaliation, threatening to target Western and Gulf critical infrastructure.

"There are now 60 hacktivist groups engaged in activities. Most neighboring countries to Iran have been targeted," CyberKnow said in a Monday message on X. "Pro-Russian groups are starting to join the fight in support of Iran and more will join in coming days."

Another post said that "Noname05716 has joined the cyber activity in support of Iran. You can expect groups part of their pro-Russian cluster to commence operations." ...

Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/us-israeli-campaign-triggers-iranian-counteroffensive-targeting-gulf-energy-critical-infrastructure/

AI-assisted credential attacks on FortiGate devices could expose OT networks to ransomware staging

The Amazon Threat Intelligence team observed a financially motivated, Russian-speaking threat actor leveraging multiple commercial generative AI services to compromise more than 600 FortiGate devices across 55 countries between Jan. 11 and Feb. 18, 2026. Rather than exploiting software vulnerabilities, the campaign succeeded by scanning for exposed management interfaces and brute-forcing weak, single-factor credentials, demonstrating how AI can empower even low-skill attackers to conduct mass intrusions.

Once inside, the actor extracted full firewall configurations, including VPN and administrative credentials and network topology data, and used this access to move into corporate environments, harvest Active Directory credentials, and target backup infrastructure — classic precursors to ransomware operations. The investigation highlights that basic security gaps, such as internet-exposed administrative ports, poor credential hygiene, and lack of multi-factor authentication, remain the primary enablers of large-scale breaches, even as commercial AI lowers the technical barrier for attackers. ...

Source and more information:

https://industrialcyber.co/vulnerabilities/ai-assisted-credential-attacks-on-fortigate-devices-could-expose-ot-networks-to-ransomware-staging/

Quantum-Resistant Data Diode Secures Sensitive Data on Edge Devices, Critical Systems

Post-quantum cryptography (PQC) roadmaps tend to focus primarily on upgrading servers and public key infrastructure (PKI), but under the radar, the need remains to protect endpoints at the edge, particularly at sites that handle sensitive data.

A new quantum-resistant data diode developed by startup Forward Edge-AI promises to protect operational technology (OT) endpoints from quantum attacks. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/quantum-resistant-data-diode-secures-sensitive-data-on-edge-devices-critical-systems

As War Continues, Pro-Iranian Actors Launch Barrage of Cyberattacks

The joint US-Israeli attack on Iran already has spurred a cyber response from multiple corners, including a barrage of distributed denial of service (DDoS) hits, critical infrastructure attacks, and network compromises that aim to do significant physical, reputational, and financial damage, according to security researchers.

On Saturday, the US and Israel launched a broad military action in Iran, killing the country's Supreme Leader Ayatollah Ali Khamenei, as well as dozens of other government officials. Iran has retaliated with both military action and cyber warfare - the latter a realm where it has more leverage against its adversaries than on the physical battlefield. ...

Source and more information:

https://www.darkreading.com/threat-intelligence/war-pro-iranian-actors-cyberattacks

The Decoupling Phase and the Capital Reckoning Behind OT Convergence

Operational Technology (OT) convergence has eliminated the historical separation between digital compromise and physical consequence. As programmable industrial systems become networked and remotely administered, a single digitally initiated event can now trigger property damage, bodily injury, environmental harm, and professional liability exposure simultaneously.

Event Horizon 3.0 examines a critical but under-discussed dimension of this convergence: capital modeling. The cyber threat economy has decoupled from insured ransom dependency, shifting toward operational leverage and infrastructure manipulation. At the same time, insurance and reinsurance capital models remain largely structured around segmented, partially independent loss assumptions. ...

Source and more information:

https://industrialcyber.co/expert/the-decoupling-phase-and-the-capital-reckoning-behind-ot-convergence/

The Availability Imperative (Why OT Security Demands Protocol-Specific Firewalls)

The world of Operational Technology (OT) demands certainty. The systems that run our factories, power grids, and water treatment plants simply cannot tolerate the unpredictable nature of standard IT gear. The core issue? Determinism. Control systems must operate with

predictable, fixed timing. Introducing security often brings the “best-effort” liability of the IT world - and that's a risk OT can't afford.

Ethernet's "Best-Effort" Problem: The Secret Behind the Standard (IEEE 802.3)

For decades, Ethernet (IEEE 802.3) has served as the bedrock of our digital world, connecting everything from corporate servers to home routers. Yet, beneath its reliable veneer lies a fundamental truth: standard Ethernet is a "best-effort" technology, which stems directly from its original media access control method, CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

[https://www.cesarkallas.net/arquivos/livros/informatica/network/Ethernet%20Definite%20Guide.pdf]. This protocol is the reason your data, while likely to arrive, is never truly guaranteed. ...

Source and more information:

The Cyber Defense eMagazine March Edition for 2026

5 Best Practices For Managing Remote Access To Industrial Equipment

There has never been a greater need for secure remote connections to production machinery. Industrial settings are getting progressively more automated and the ability to issue commands and troubleshoot without being on-site in the midst of potential hazards is crucial for proactive operations. How can teams best handle and supervise remote access in these environments?

1. Implement Zero-Trust Architecture (ZTA)

ZTA sets a precedent in digital systems. Every access attempt demands verification and never assumes trust. This infrastructure comprises many moving parts, including multifactor authentication, secure shell keys, segmentation and other validation measures. ...

Source and more information:

The Cyber Defense eMagazine March Edition for 2026

NIST Urged to Go Deep in OT Security Guidance

Now is the moment for U.S. federal guidance on securing operational technology to plunge deeper into the practicalities of securing systems, an extension into actionable advice that reflects a maturing branch of cybersecurity, several OT security specialists told the National Institute of Standards and Technology.

NIST announced in January it was embarking on the fourth rewrite of its OT security guidance, known as Special Publication 800-82 and asked for input from the private sector and others.

"The more granular and specific these frameworks and guidelines can get, the more helpful it is," Dragos Vice President of Public Policy and Government Affairs Kate Diemidio told Information Security Media Group. ...

Source and more information:

https://www.ot.today/nist-urged-to-go-deep-in-ot-security-guidance-a-30933

Webinar Today: Designing an OT SOC for Safety, Reliability, and Business Continuity

Join the webinar as we explore a blueprint for an OT SOC leveraging an integrated OT Security Platform to safeguard operations and maintain business continuity.

Industrial Cybersecurity Webinar – Wednesday, March 4, 2026 at 1PM ET – Register to Attend

Industrial organizations face an escalating wave of cyberattacks targeting operational technology (OT) environments that are now focused on not only disrupting operations but providing attack vectors for later use. This is driving the need for security operations that extend beyond traditional IT boundaries. As cyber-physical systems become increasingly interconnected with IT, cloud platforms, and multiple third parties, the priority shifts from reactive visibility to proactive defense and incident management.

Protecting physical safety, production uptime, and revenue against sophisticated threats requires OT security operations integrated into the enterprise Network and Security Operations Center (NOC/SOC).

By aligning with regulatory and compliance standards, an OT SOC delivers continuous visibility and resilience across critical infrastructure sectors. …

Source and more information:

https://www.securityweek.com/webinar-today-designing-an-ot-soc-for-safety-reliability-and-business-continuity/

Kai Emerges From Stealth With $125M in Funding for AI Platform Bridging IT and OT Security

Kai on Tuesday emerged from stealth mode with $125 million in funding for an AI-powered platform that aims to bridge IT and OT cybersecurity.

The investment, raised over seed and Series A funding rounds, comes from Evolution Equity Partners, N47, and other investors.

The funding will be used for R&D, scaling the company's platform, and accelerating go-to-market efforts.

San Jose, CA-based Kai was founded by Galina Antova (CEO) and Damiano Bolzoni (CTO). Antova (a former SecurityWeek contributor) previously co-founded OT security giant Claroty, while Bolzoni co-founded SecurityMatters, an OT security firm that was acquired by Forescout Technologies in 2018. …

Source and more information:

https://www.securityweek.com/kai-emerges-from-stealth-with-125m-in-funding-for-ai-platform-bridging-it-and-ot-security/

Stop fixing OT security with IT thinking

In this Help Net Security interview, Ejona Preçi, Group CISO at Lindal Group, discusses the specific cybersecurity challenges in manufacturing environments. The conversation covers why standard IT security practices break down on shop floors, where PLCs and decade-old firmware were never designed to be networked.

She explains how nation-state actors quietly settle into industrial networks, using stale accounts and compromised workstations to map environments without triggering alarms. She addresses patch management in OT, where production lines cannot simply be taken offline, and describes how security teams use compensating controls to manage risk without breaking operations. The interview also examines how adding sensors and telemetry can generate noise that hides real threats, and how AI pipelines connecting IT and OT systems create new attack surfaces. …

Source and more information:

https://www.helpnetsecurity.com/2026/03/12/ejona-preci-lindal-group-ot-cybersecurity-manufacturing/

Data Diodes Have Become Essential to Modern OT Cybersecurity

In an enterprise security landscape dominated by firewalls, antivirus software, intrusion detection systems and relentless artificial intelligence hype, the quiet efficacy of data diodes has left them largely absent from mainstream discussion.

But this overlooked technology has long been a staple of secure network architecture and segmentation in critical environments. A data diode is a hardware network appliance designed to enforce unidirectional data transfer. …

Source and more information:

https://www.ot.today/blogs/data-diodes-have-become-essential-to-modern-ot-cybersecurity-p-4063

Building 'Incident Management for Industrial Control Systems' to address gaps in OT cyber incident response

Industrial cybersecurity programs have matured considerably in the past 10 years, with many organizations spending substantial sums on detection tools, network segmentation, and preventive controls. Yet when they happen, response capabilities are locked behind these defenses. Playbooks are lacking, roles are undefined, and collaboration between cybersecurity teams, plant operators and leadership is seldom practiced in industry. In the industry, where

an interruption can be so quickly translated into risk to safety or a stopped production line, improvisation is minimal. It is these gaps that led OT and cybersecurity risk management veteran Durgesh Kalya to pen Incident Management for Industrial Control Systems. ...

Source and more information:

https://industrialcyber.co/interview/building-incident-management-for-industrial-control-systems-to-address-gaps-in-ot-cyber-incident-response/

Poland's nuclear research centre targeted by cyberattack

Poland's National Centre for Nuclear Research (NCBJ) says hackers targeted its IT infrastructure, but the attack was detected and blocked before causing any impact.

In a statement this week, the organization announced that its security systems and internal procedures, designed to detect threats early, prevented the compromise and allowed its IT staff to quickly secure targeted systems.

"Thanks to the rapid and effective actions of security systems and procedures in the event of such an incident, as well as the quick response of our teams, the attack was thwarted, and the integrity of the systems was not compromised," the NCBJ says. ...

Source and more information:

https://www.bleepingcomputer.com/news/security/polands-nuclear-research-centre-targeted-by-cyberattack/

New York introduces cybersecurity rules, $2.5 million grant program to strengthen water infrastructure defenses

New cybersecurity regulations for drinking water and wastewater systems have been announced in New York, alongside a US$2.5 million grant program designed to help communities strengthen cyber defenses for critical water infrastructure. Led by Governor Kathy Hochul, the Strengthening Essential Cybersecurity for Utilities and Resiliency Enhancements grant program, administered by the New York State Environmental Facilities Corporation, provides funding of up to $50,000 for cybersecurity assessments and up to $100,000 for utilities to implement cybersecurity upgrades. These grants are meant for system improvements to help utilities strengthen defenses against increasingly sophisticated cyber threats. ...

Source and more information:

https://industrialcyber.co/utilities-energy-power-water-waste/new-york-introduces-cybersecurity-rules-2-5-million-grant-program-to-strengthen-water-infrastructure-defenses/

Beyond CVSS: OT Security Looks for Its Risk Methodology

A mainstay of IT security programs across the world, the Common Vulnerability Scoring System, may have terminal flaws when applied to the mirror universe of operational technology - a place where ordinary assumptions about risk don't apply.

OT have long argued that CVSS is an inadequate measure for their purposes. In November 2023, the Forum of Incident Response and Security Teams, which maintains CVSS, sought to address those complaints with a new version, CVSS 4.0.

But a growing number of OT security experts believe it's becoming clear that CVSS can't be "fixed" - even putting aside issues such as the administrative burden required to implement CVSS 4.0 in the OT world. ...

Source and more information:

https://www.ot.today/beyond-cvss-ot-security-looks-for-its-risk-methodology-a-31038

Claroty reports 82% of CPS attacks used remote access protocols as hacktivists target HMIs and SCADA at scale

Claroty's Team82 disclosed that cybercriminals are increasingly targeting global critical infrastructure by directly accessing exposed cyber-physical systems, highlighting a fast-escalating threat to industrial control environments. Analysis of over 200 incidents over the past year revealed that 82% of attacks leveraged remote access protocols to reach internet-facing assets, and 66% involved the compromise of HMIs (Human Machine Interfaces) and SCADA systems that control essential processes across sectors such as energy, water, manufacturing and healthcare.

The research found politically and socially motivated threat actors, particularly those linked to Russia and Iran, are exploiting low-tech but widely exposed systems, underscoring growing risks to public safety and service continuity. ...

Source and more information:

https://industrialcyber.co/reports/claroty-reports-82-of-cps-attacks-used-remote-access-protocols-as-hacktivists-target-hmis-and-scada-at-scale/

Mitsubishi Deal Gives Nozomi Broader OT Security Reach

Becoming part of Mitsubishi will help Nozomi Networks find uses for industrial data beyond cybersecurity, including for preventative maintenance and operational efficiency, according to CEO Edgard Capdevielle.

Mitsubishi's technical collaboration capabilities make it an ideal parent company and helps Nozomi avoid the uncertainty typical of venture-backed companies. Capdevielle said Mitsubishi will provide stability, scale and alignment without sacrificing independence, helping

Nozomi expand into broader use cases around asset management, maintenance and efficiency (see: Mitsubishi Electric to Buy Nozomi in $883M OT Security Deal). ...

Source and more information:

https://www.ot.today/mitsubishi-deal-gives-nozomi-broader-ot-security-reach-a-31076

DOE Sets 5-Year Plan to Harden US Grid Against Cyberattacks

The U.S. Department of Energy released a first-ever comprehensive strategy for securing the nation's energy infrastructure, laying out a five-year roadmap that aims to translate broad White House cyber priorities into concrete action.

The plan, published Wednesday by the Office of Cybersecurity, Energy Security and Emergency Response, outlines how the government intends to strengthen grid resilience, accelerate the development of security technologies and improve the sector's ability to respond to and recover from cyber incidents. Officials describe it as the office's first formal effort to define its mission, goals and measurable outcomes in a single document. ...

Source and more information:

https://www.ot.today/doe-sets-5-year-plan-to-harden-us-grid-against-cyberattacks-a-31124

Crisis lessons from OT incident response as cyber-physical attacks unfold within normal industrial operations

Industrial cyber threats and attacks are rarely announced by blaring sirens warning organizations of their impending threats or danger. Instead, they look like mundane processing activities until a valve opens prematurely, a controller receives an order it should never obey, or operators detect a disconnect between how the plant is operating and how it should be operating. That is what cyber-physical attacks look like in OT environments, where the adversaries lurk inside the organizations and escalate quickly into safety and operational incidents.

OT incident response is very different when compared to IT compromises or attacks. In many industrial applications, the priorities lie in organizational safety, reliability, and availability, before confidentiality. A compromised PLC or control loop can wreak havoc in minutes, producing equipment destruction or even human injury, making conventional responses, such as immediate isolation or aggressive scanning, could result in unsafe process conditions, rather than containing risk. Incident response emerges as a delicate balance that organizations need to strike to neutralize the threat while remaining stable to continue operations. ...

Source and more information:

https://industrialcyber.co/features/crisis-lessons-from-ot-incident-response-as-cyber-physical-attacks-unfold-within-normal-industrial-operations/

How Cyberattacks Can Turn Battery Farms Into Grid Blackouts

Decentralized energy systems are now essential parts of energy grids as power demands for artificial intelligence-enabled data centers skyrockets. But cybersecurity for these systems hasn't kept pace, leaving battery energy storage resources exposed as they play a growing role in grid stability, said Rafael Narezzi, CEO at Centrii.

In fact, in December 2025 in Poland, cyberattackers demonstrated how they can disrupt grid balancing rather than halt production outright. The lesson for the energy sector is that weak controls in decentralized systems can quickly go from a localized disruption to major problems affecting the entire grid, he said. ...

Source and more information:

https://www.ot.today/how-cyberattacks-turn-battery-farms-into-grid-blackouts-a-31191

Rising ICS incidents drive shift from reactive risk models to intelligence-driven OT security strategies

Traditional organizational risk models are struggling to cope with the changing industrial threat scenario, as the former have been designed for static environments rather than dynamic, converged operational networks. In a scenario where ICS and SCADA systems integrate with enterprise IT systems, traditional security models are not able to cope. There has been a 49% increase in attacks by state-aligned adversaries on energy, transport, and water sectors during 2024. The urgency of the situation is also clear from the fact that the security of OT systems is a US$27.03 billion market in 2025 and is expected to grow to $122.22 billion by 2034. ...

Source and more information:

https://industrialcyber.co/threats-attacks/rising-ics-incidents-drive-shift-from-reactive-risk-models-to-intelligence-driven-ot-security-strategies/

Lesson From Enigma Cipher Machine Shapes OT Sec Strategy

Lessons from the breaking of the German Enigma cypher machine code during World War II reveal many of the risks facing operational technology security teams today. Engineering flaws and operator errors - not weak encryption - enabled British researchers to exploit one of the most advanced systems of its time and turn the tide in the war.

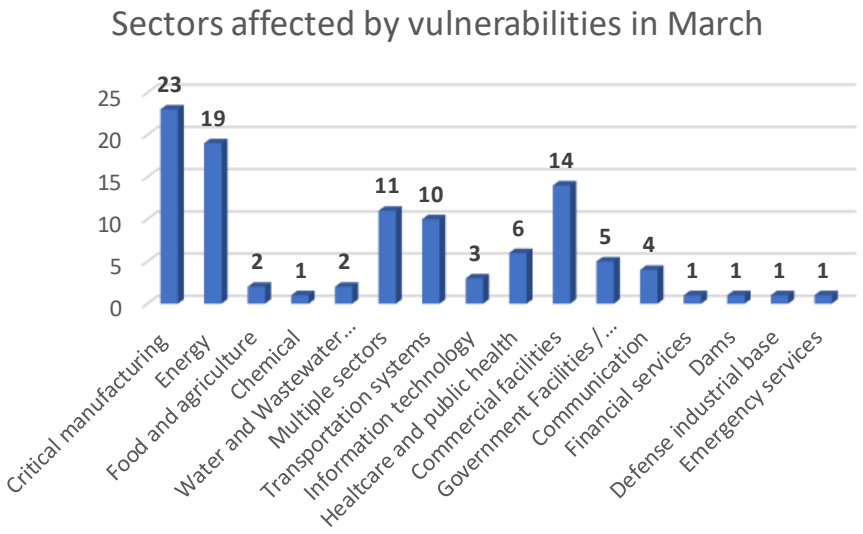
Today, cyberattackers use remote access, internet connectivity and software vulnerabilities to gain a foothold in OT environments and move laterally to compromise enterprises. "We think we're doing everything right, and our adversary finds that one little thing we forgot," said Marcus Sachs, senior vice president and chief engineer at the Center for Internet Security. ...

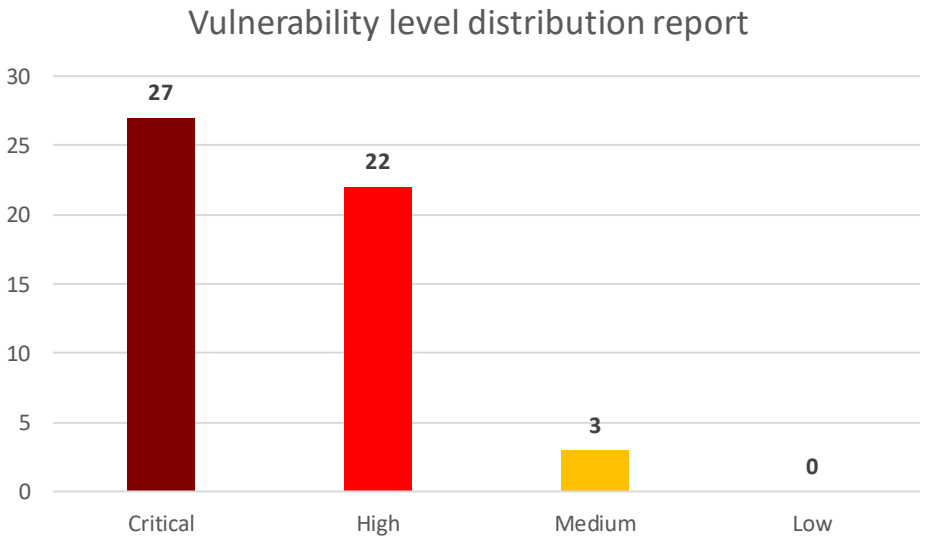
Source and more information:

https://www.ot.today/lesson-from-enigma-cipher-machine-shapes-ot-sec-strategy-a-31251

6. ICS vulnerabilities

In March 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-26-085-01: **WAGO GmbH & Co. KG Industrial Managed Switches**

Critical level vulnerability: Hidden Functionality.

WAGO GmbH & Co. KG Industrial Managed Switches | CISA

ICSA-26-085-02: **OpenCode Systems OC Messaging and USSD Gateway**

High level vulnerability: Improper Access Control.

OpenCode Systems OC Messaging and USSD Gateway | CISA

ICSA-26-085-03: **PTC Windchill Product Lifecycle Management**

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

PTC Windchill Product Lifecycle Management | CISA

ICSA-26-069-03: **Honeywell IQ4 Series BMS Controller (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Honeywell IQ4x BMS Controller (Update A) | CISA

ICSMA-26-083-01: **Grassroots DICOM (GDCM)**

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

Grassroots DICOM (GDCM) | CISA

ICSA-26-083-01: **Pharos Controls Mosaic Show Controller**

Critical level vulnerability: Missing Authentication for Critical Function.

Pharos Controls Mosaic Show Controller | CISA

ICSA-26-083-03: **Schneider Electric Plant iT/Brewmaxx**

Critical level vulnerabilities: Use After Free, Integer Overflow or Wraparound, Improper Control of Generation of Code ('Code Injection').

Schneider Electric Plant iT/Brewmaxx | CISA

ICSMA-25-364-01: **WHILL Model C2 Electric Wheelchairs and Model F Power Chairs (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

WHILL Model C2 Electric Wheelchairs and Model F Power Chairs (Update A) | CISA

ICSA-26-078-03: **Schneider Electric EcoStruxure Automation Expert**

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

Schneider Electric EcoStruxure Automation Expert | CISA

ICSA-26-078-04: **Schneider Electric EcoStruxure Power**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure PME and EPO | CISA

ICSA-26-078-06: **CTEK Chargeportal**

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

CTEK Chargeportal | CISA

ICSA-26-078-07: **IGL-Technologies eParking.fi**

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

IGL-Technologies eParking.fi | CISA

ICSA-26-078-08: **Automated Logic WebCTRL Premium Server**

Critical level vulnerabilities: Multiple Binds to the Same Port, Authentication Bypass by Spoofing, Cleartext Transmission of Sensitive Information.

Automated Logic WebCTRL Premium Server | CISA

ICSA-26-076-01: **CODESYS in Festo Automation Suite**

Critical level vulnerabilities: Direct Request ('Forced Browsing'), Untrusted Search Path, Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Recursion, Improper Access Control, Use of Insufficiently Random Values, Improper Restriction of Communication Channel to Intended Endpoints, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), NULL Pointer Dereference, Stack-based Buffer Overflow, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Incorrect Permission Assignment for Critical Resource, Improper Handling of Exceptional Conditions, Exposure of Resource to Wrong Sphere, Allocation of Resources Without Limits or Throttling, Use of a Broken or Risky Cryptographic Algorithm, Out-of-bounds Write, Weak Password Recovery Mechanism for Forgotten Password, Improper Privilege Management, Use of Password Hash With Insufficient Computational Effort, Buffer Access with Incorrect Length Value, Improper Input Validation, Improper Verification of Cryptographic Signature, Inadequate Encryption Strength, Origin Validation Error, Missing Release of Memory after Effective Lifetime, Improper Resource Shutdown or Release, Deserialization of Untrusted Data, Path Equivalence: '//multiple/leading/slash', Insufficient Verification of Data Authenticity, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Missing Authentication for Critical Function, Out-of-bounds Read, Failure to Sanitize Special Elements into a Different Plane (Special Element Injection), Use of Out-of-range Pointer Offset, Improper Neutralization of Script in Attributes of IMG Tags in a Web Page, Files or Directories Accessible to External Parties, Untrusted Pointer Dereference, Path Traversal: '....' (Multiple Dot), ASP.NET Misconfiguration: Missing Custom Error Page, Uncontrolled Resource Consumption, Unprotected Transport of Credentials, Initialization of a Resource with an Insecure Default, Heap-based Buffer Overflow, Unexpected Sign Extension, Buffer Over-read, Uncontrolled

Search Path Element, Improper Verification of Source of a Communication Channel, Improper Restriction of Excessive Authentication Attempts, Use After Free, ASP.NET Misconfiguration: Password in Configuration File, Improper Check for Unusual or Exceptional Conditions, Observable Discrepancy, Incorrect Default Permissions.

CODESYS in Festo Automation Suite | CISA

ICSA-26-076-02: **Schneider Electric SCADAPack and RemoteConnect**

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

Schneider Electric SCADAPack and RemoteConnect | CISA

ICSA-26-076-03: **Schneider Electric EcoStruxure IT Data Center Expert**

High level vulnerability: Use of Hard-coded Credentials.

Schneider Electric EcoStruxure Data Center Expert | CISA

ICSA-26-076-04: **Siemens SICAM SIAPP SDK**

High level vulnerabilities: Out-of-bounds Write, Stack-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency, External Control of File Name or Path.

Siemens SICAM SIAPP SDK | CISA

ICSA-25-160-02: **Hitachi Energy's Relion 670, 650, SAM600-IO series (Update A)**

Medium level vulnerability: Observable Discrepancy.

Hitachi Energy Relion 670, 650, SAM600-IO Series (Update A) | CISA

ICSA-26-015-10: **Schneider Electric EcoStruxure Power Build Rapsody (Update A)**

High level vulnerabilities: Double Free, Use After Free.

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

SSA-868571: **Missing Server Certificate Validation in IAM Client (Update: 1.1.)**

Critical level vulnerability: Improper Certificate Validation.

SSA-868571

SSA-770770: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.7 on RUGGEDCOM APE1808 Devices (Update: 1.8.)**

Critical level vulnerabilities: Multiple.

SSA-770770

SSA-710408: **Missing Server Certificate Validation in Siemens Advanced Licensing (SALT) Toolkit (Update: 1.1.)**

Critical level vulnerability: Improper Certificate Validation.

SSA-710408

SSA-535115: **Data Validation Vulnerability in NX Before V2512 (Update: 1.1.)**

High level vulnerability: Stack-based Buffer Overflow.

SSA-535115

SSA-513708: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices (Update: 1.4.)**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Exposure of Sensitive System Information to an Unauthorized Control Sphere, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Script in Attributes in a Web Page, Improper Check for Unusual or Exceptional Conditions, Improper Certificate Validation.

SSA-513708

SSA-430425: **Multiple Vulnerabilities in SINEC Security Monitor before V4.9.0 (Update: 1.1.)** **Critical** level vulnerabilities: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), Improper Neutralization of Special Elements used in a Command ('Command Injection'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Permissive List of Allowed Inputs, Exposure of Sensitive Information Through Metadata.

SSA-430425

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update: 1.7.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-212953: **Multiple Vulnerabilities in COMOS (Update: 1.3.)**

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

SSA-212953

SSA-201595: **Privilege Escalation Vulnerability in WIBU CodeMeter Runtime Affecting the Desigo CC Product Family and SENTRON Powermanager (Update: 1.3.)**

High level vulnerability: Least Privilege Violation.

SSA-201595

SSA-082556: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1.5 (Update: 1.4.)**

High level vulnerabilities: Multiple.

SSA-082556

SSA-027652: **Privilege Escalation Vulnerability in SINAMICS Drives (Update: 1.1.)**

Medium level vulnerability: Improper Privilege Management.

SSA-027652

ICSA-26-071-01: **Trane Tracer SC, Tracer SC+, and Tracer Concierge**

High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Memory Allocation with Excessive Size Value, Missing Authorization, Use of Hard-coded Credentials, Use of Hard-coded, Security-relevant Constants.

Trane Tracer SC, Tracer SC+, and Tracer Concierge | CISA

ICSA-26-071-02: **Siemens RUGGEDCOM APE1808**

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

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-26-071-03: **Siemens SIDIS Prime**

High level vulnerabilities: Out-of-bounds Read, Observable Discrepancy, Improper Input Validation, Improper Certificate Validation, Numeric Truncation Error, Use of Insufficiently Random Values, Out-of-bounds Write, Inefficient Regular Expression Complexity, Interpretation Conflict, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Relative Path Traversal, Allocation of Resources Without Limits or Throttling, Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Integer Overflow or Wraparound, Uncontrolled Recursion, Insertion of Sensitive Information Into Sent Data, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incomplete List of Disallowed Inputs.

Siemens SIDIS Prime | CISA

ICSA-26-071-04: **Siemens SIMATIC**

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

Siemens SIMATIC | CISA

ICSA-26-048-04: **Honeywell HIB2PI CCTV Camera (Update B)**

Critical level vulnerability: Missing Authentication for Critical Function.

Honeywell HIB2PI and HDZ Series CCTV Cameras (Update B) | CISA

ICSA-26-069-01: **Apeman Cameras**

Critical level vulnerabilities: Insufficiently Protected Credentials, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authentication for Critical Function.

Apeman Cameras | CISA

ICSA-26-069-02: **Lantronix EDS3000PS and EDS5000**

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 | CISA

ICSA-26-069-03: **Honeywell IQ4x BMS Controller**

Critical level vulnerability: Missing Authentication for Critical Function.

Honeywell IQ4x BMS Controller | CISA

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

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

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

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

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

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

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

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

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

ICSA-26-064-01: **Delta Electronics CNCSoft-G2**

High level vulnerability: Out-of-bounds Write.

Delta Electronics CNCSoft-G2 | CISA

ICSA-25-343-01: **Universal Boot Loader (U-Boot) (Update A)**

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

Universal Boot Loader (U-Boot) (Update A) | CISA

ICSA-25-350-02: **Johnson Controls PowerG, IQPanel and IQHub (Update A)**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Reusing a Nonce, Key Pair in Encryption, Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Origin Validation Error.

Johnson Controls PowerG, IQPanel and IQHub (Update A) | CISA

ICSA-26-062-02: **Hitachi Energy Relion REB500**

Medium level vulnerability: Privilege Defined With Unsafe Actions.

Hitachi Energy Relion REB500 Product | CISA

ICSA-26-062-03: **Hitachi Energy RTU500 Product**

High level vulnerabilities: Improper Handling of Insufficient Permissions or Privileges , Incomplete List of Disallowed Inputs, Uncontrolled Recursion, Allocation of Resources Without Limits or Throttling.

Hitachi Energy RTU500 Product | CISA

ICSA-26-062-04: **Portwell Engineering Toolkits**

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

Portwell Engineering Toolkits | CISA

ICSA-26-062-05: **Labkotec LID-3300IP**

Critical level vulnerability: Missing Authentication for Critical Function.

Labkotec LID-3300IP | CISA

ICSA-26-062-06: **Mobiliti e-mobi.hu**

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

Mobiliti e-mobi.hu | CISA

ICSA-26-062-07: **ePower epower.ie**

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

ePower epower.ie | CISA

ICSA-26-062-08: **Everon api.everon.io**

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

Everon OCPP Backends | CISA

ICSA-25-023-02: **Hitachi Energy RTU500 Series Product (Update B)**

High level vulnerability: Improperly Implemented Security Check for Standard.

Hitachi Energy RTU500 Series Product (Update B) | CISA

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

ICS Advisories | CISA

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

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

7. ICS alerts

CISA has published alerts in 2026 March:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2026-21385 Qualcomm Multiple Chipsets Memory Corruption Vulnerability;
CVE-2026-22719 Broadcom VMware Aria Operations Command Injection Vulnerability;
CVE-2017-7921 Hikvision Multiple Products Improper Authentication Vulnerability;
CVE-2021-22681 Rockwell Multiple Products Insufficient Protected Credentials Vulnerability;
CVE-2021-30952 Apple Multiple Products Integer Overflow or Wraparound Vulnerability;
CVE-2023-41974 Apple iOS and iPadOS Use-After-Free Vulnerability;
CVE-2023-43000 Apple Multiple products Use-After-Free Vulnerability;
CVE-2021-22054 Omnissa Workspace ONE Server-Side Request Forgery;
CVE-2025-26399 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability;
CVE-2026-1603 Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability;
CVE-2025-68613 n8n Improper Control of Dynamically-Managed Code Resources Vulnerability;
CVE-2026-3909 Google Skia Out-of-Bounds Write Vulnerability;
CVE-2026-3910 Google Chromium V8 Unspecified Vulnerability;
CVE-2025-47813 Wing FTP Server Information Disclosure Vulnerability;
CVE-2025-66376 Synacor Zimbra Collaboration Suite (ZCS) Cross-Site Scripting Vulnerability;
CVE-2026-20131 Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability;
CVE-2026-33017 Langflow Code Injection Vulnerability;
CVE-2026-33634 Aqua Security Trivy Embedded Malicious Code Vulnerability;
CVE-2025-53521 F5 BIG-IP Remote Code Execution Vulnerability;
CVE-2026-3055 Citrix NetScaler Out-of-Bounds Read Vulnerability;

Links and more information:

CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds 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

Russian Intelligence Services Target Commercial Messaging Application Accounts

CISA and the Federal Bureau of Investigation released a Public Service Announcement (PSA) warning about ongoing phishing campaigns by cyber actors associated with the Russian Intelligence Services targeting commercial messaging applications (CMAs). These campaigns aim to bypass encryption to compromise to individual user accounts with targets including current and former U.S. government officials, military personnel, political figures, and journalists.

Links and more information:

Russian Intelligence Services Target Commercial Messaging Application Accounts | CISA

8. ICS trainings, education

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

9. ICS podcasts

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

Dale Peterson

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

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

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

Industrial Cybersecurity Pulse

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

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

BEERISAC: OT/ICS Security Podcast Playlist

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

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

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