2025 October, 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

ICS good practices, recommendations

Hardening ICS/OT Environments with CIS Security Controls

In managing cybersecurity, organizations benefit from adopting recognized frameworks that offer structured, prioritized approaches to protection. For Operational Technology (OT) environments, frameworks such as NERC CIP and the CIS Controls are widely used - some focusing on regulatory compliance, others emphasizing practical security improvement.

The CIS Critical Security Controls (CIS Controls), developed by the Center for Internet Security, form a concise, prioritized set of best practices designed to stop the most common and dangerous cyberattacks. It consists of 18 specific controls, each representing a focused defensive action that collectively ensures robust cybersecurity hygiene. These include asset and software inventory, data protection, secure configuration, access and account management, continuous vulnerability management, audit logging, malware defenses, data recovery, network management, incident response, and penetration testing.

Adopting CIS Controls helps organizations of any size to create a prescriptive, cost-effective roadmap for cybersecurity, enabling them to prioritize resources efficiently. Many companies use them as both a standard and a planning tool, aligning technical initiatives and security budgets with measurable outcomes.

While CIS Controls were initially designed for IT systems, their relevance in Industrial Control Systems (ICS) and OT has grown significantly due to the increasing threat landscape targeting critical infrastructure. OT systems, which directly control physical processes such as electricity, water, or fuel delivery, require a balance between security and availability. Recognizing this, CIS developed an ICS Companion Guide to adapt its controls to the specific constraints and operational realities of industrial environments.

Implementing CIS Controls in OT settings demands attention to vendor dependencies, system warranties, and operational continuity. Many OT asset owners depend on vendor-specific technologies that may limit modification capabilities; therefore, careful coordination is required to enhance security without disrupting critical operations.

To effectively operate CIS Controls, organizations should leverage tools that provide deep visibility into OT assets, including system states, configurations, and vulnerabilities. Solutions like Industrial Defender enable automated compliance reporting, baseline monitoring, and drift detection - ensuring continuous alignment with CIS requirements.

Ultimately, CIS Controls offer a practical, adaptable, and recognized framework for improving OT cybersecurity maturity, strengthening resilience, and demonstrating a reasonable level of protection across industries.

Source, links and more detailed information available on the following link:

https://www.industrialdefender.com/blog/hardening-ics-ot-environments-with-cis-security-controls

ICS conferences

In November 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

DRAGOS INDUSTRIAL SECURITY CONFERENCE

Your opportunity to network with the industrial asset owner and operator community while learning the latest technical, in-depth research findings and insights from Dragos experts and ICS/OT practitioners on the frontlines.

Hanover, Maryland; 4th – 6th November 2025

More details can be found on the following website:

https://events.dragos.com/disc2025

Industrial Security Conference Copenhagen

"We have a place we meet in Asia, a place we meet in the US, and now we have a place in Europe," stated Saltanat Mashirova, Product Management Lead, Connected Cybersecurity, Honeywell. ISC-CPH 2025, taking place on November 10 - 12, will be a three-day international event dedicated to advancing industrial cybersecurity. The first day will feature two focused tracks - one for the manufacturing sector and one for utilities and energy - addressing their distinct challenges and regulatory landscapes. In addition to keynote sessions and presentations, the agenda includes in-depth workshops for practical skill development. Recognized as one of Europe's fastest-growing industrial security conferences, ISC-CPH provides a platform for professionals to exchange expertise, build partnerships, and enhance the protection of critical infrastructure.

Copenhagen, Denmark; 10th – 12th November 2025

More details can be found on the following website:

https://insightevents.dk/isc-cph/

20th Annual API Cybersecurity Conference for the Oil and Natural Gas Industry

The API Cybersecurity Conference has been an annual event since 2005. For 20 years it has been the only cybersecurity conference dedicated to the oil and natural gas industry and has a loyal and dedicated attendee base. It is also volunteer-driven, both at the planning committee and speaker level. The organizers consistently produce a compelling conference program, with a focus on safety, best practices, and innovation. In addition, the conference provides an opportunity for attendees to earn CPEs (Continuing Professional Education), maintaining their certifications and required hours. Finally, the conference provides the opportunity for networking and idea exchange, with our dedicated sponsors and exhibitors sharing their latest products and services.

The Woodlands, Texas, USA; 11th – 12th November 2025

More details can be found on the following website:

https://events.api.org/20th-annual-api-cybersecurity-conference-for-the-oil-and-natural-gas-industry/

Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region

The program, which takes place in Tokyo each year, aims to improve ICS cybersecurity for critical infrastructure providers, manufacturers, and others from the Indo-Pacific region.

The one-week training program for the Indo-Pacific region is organised by the governments of Japan, the U.S., and the EU. It has been held annually since 2018.

The training will include hands-on exercises using special facilities in Japan, lectures by subject matter experts from Japan, the US, and the EU, and opportunities for networking among participants.

Tokyo, Japan; 18th -21st November 2025

More details can be found on the following website:

https://www.icscybersecurityweek.info/

ICS incidents

Brewer Asahi suspends domestic operations after cyberattack disrupts ordering and shipping

Asahi Group Holdings, Japan's largest brewing company, has suspended ordering, shipping, and customer service operations in Japan following a cyberattack that disrupted domestic systems. The company, known internationally for its Asahi Super Dry beer and other beverages, stated that no confirmed leakage of personal or customer data has been identified. However, order processing, shipments, and call center functions remain suspended. An internal investigation is underway, with no timeline announced for recovery. The disruption is currently limited to operations within Japan.

The incident comes amid rising cyber risks across Japanese industry. A 2022 Teikoku Databank survey found that 36.1% of companies experienced a cyberattack in the past year, with nearly 30% reporting incidents within the previous month. In parallel, Japan has adopted the new Active Cyber Defense Law, expanding its cybersecurity framework by mandating incident reporting for critical infrastructure and granting government authority to intercept foreign internet traffic crossing domestic networks. Response actions are to be carried out by the National Police Agency or Self-Defense Forces.

Operational disruptions due to cyberattacks are becoming more common worldwide. Jaguar Land Rover recently extended a production halt into October after an August attack, while Bridgestone confirmed a September cyber incident that temporarily impacted North American manufacturing facilities before containment and recovery.

Research by BitSight indicates that industrial control systems (ICS) and operational technology (OT) exposures to the public internet are again on the rise, increasing 12 percent in 2024 to more than 180,000 devices detected monthly, with levels expected to approach 200,000 in 2025.

In the food and agriculture sector, collaborative defenses are strengthening. The Food and Agriculture Information Sharing and Analysis Center (Food and Ag-ISAC) announced the American Farm Bureau Federation has joined its Industry Association Partner Program, enhancing access to threat intelligence, incident alerts, and cybersecurity best practices for members.

The Asahi incident underscores the vulnerability of critical production and supply chain operations to cyber threats, as well as the growing need for regulatory action and cross-sector collaboration in response.

The source is available at the following link:

https://industrialcyber.co/manufacturing/brewer-asahi-suspends-domestic-operations-after-cyberattack-disrupts-ordering-and-shipping/

Update:

Japanese brewery and food conglomerate Asahi Group Holdings recently suffered a ransomware attack that forced a full shutdown of its manufacturing and logistics operations, leading to nationwide shortages of its beer products. The attack, claimed by the Qilin ransomware group, disrupted Asahi's ordering, shipping, and call-center systems, demonstrating the significant operational impact ransomware can have on manufacturing environments.

The incident underscores a growing cyber risk to operational technology (OT) in the manufacturing sector. As organizations increasingly interconnect their IT and OT networks for automation and efficiency, weak or missing network segmentation allows attackers to move laterally from corporate systems into production environments. Once operational systems are encrypted, production halts become inevitable, directly affecting revenue and supply chains.

Experts note that manufacturers are particularly vulnerable due to thin profit margins and historically underfunded cybersecurity investments. According to Sophos, over 850 ransomware attacks have targeted manufacturers in recent years, with estimated losses of $1.9 million per day of downtime.

Qilin, currently one of the most active ransomware groups, has made the manufacturing sector its primary target, responsible for over 20% of its attacks in early 2024. The Asahi case illustrates how such attacks not only threaten data confidentiality but also disrupt physical production, exposing the critical interdependence between IT and OT security.

Japan's new Active Cyber Defense law may strengthen national response capabilities, but experts warn that ransomware remains a rapidly evolving and persistent threat, demanding stronger cyber resilience and OT network protection at the organizational level.

The source is available at the following link:

https://www.darkreading.com/ics-ot-security/cyberattack-beer-shortage-asahi-recovers

Book recommendation

Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems 3rd Edition

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems - energy production, water, gas, and other vital systems - becomes more important, and heavily mandated. Industrial Network Security, Third Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems.

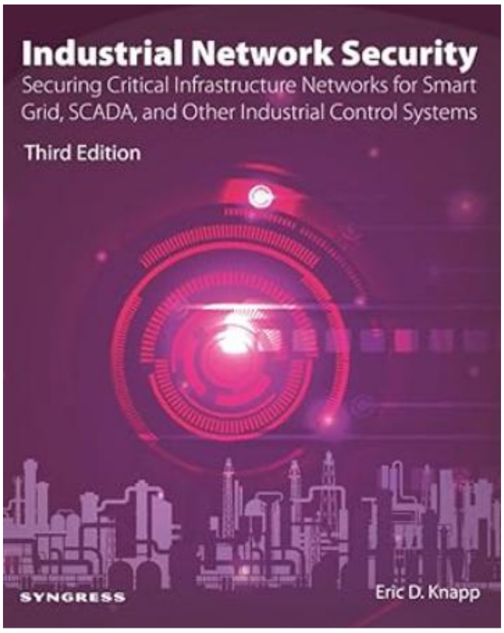
Author Eric Knapp examines the unique protocols and applications that are the foundation of Industrial Control Systems (ICS) and provides clear guidelines for their protection. This comprehensive reference gives you thorough understanding of the challenges facing critical infrastructures, new guidelines and security measures for infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation.

Author/Editor: Eric D. Knapp (Author)

Year of issue: 2024

The book is available at the following link:

https://www.amazon.com/Industrial-Network-Security-Securing-Infrastructure/dp/0443137374?utm_source=chatgpt.com


Industrial Network Security
Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems
Third Edition
SYNGRESS
Eric D. Knapp

ICS security news selection

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

1. **Siemens simplifies OT security with virtualized, encrypted connectivity**
2. **NIST Publishes Guide for Protecting ICS Against USB-Borne Threats**
3. **The Phantom Slice (How Silent Protocol Exploits In 5g Are Creating A Ticking Time Bomb In Critical Infrastructure)**
4. **Many Attacks Aimed at EU Targeted OT, Says Cybersecurity Agency**
5. **Researchers track Cavalry Werewolf custom malware attacks on Russian government, industrial networks**
6. **Radiflow360 unifies OT risk, compliance, and response**
7. **The five-minute guide to OT cyber resilience**
8. **A safer way to break industrial systems (on purpose)**
9. **The Fight Against Ransomware Heats Up on the Factory Floor**
10. **As industrial systems modernize, adaptive OT cybersecurity replaces patchwork defense**
11. **New Microchip Tech Protects Vehicles from Laser Attacks**
12. **Fuji Electric HMI Configurator Flaws Expose Industrial Organizations to Hacking**
13. **Electronic Warfare Puts Commercial GPS Users on Notice**
14. **Forescout warns TP-Link router vulnerabilities could expose industrial systems, provides mitigations**
15. **CSIS: USCG poised for ‘generational change’ in maritime cybersecurity with new tools, $25B funding**
16. **Canada’s Cyber Centre urges action as Internet-accessible ICS face growing cyber threats from hacktivists**
17. **Industrial Giants Schneider Electric and Emerson Named as Victims of Oracle Hack**

Siemens simplifies OT security with virtualized, encrypted connectivity

Siemens launched SINEC Secure Connect, the zero trust security platform designed for operational technology (OT) networks. The software solution virtualizes network structures using overlay networks. It enables Machine-to-Machine, Machine-to-Cloud, and Machine-to-Datacenter connections, plus secure remote access to industrial systems, all without relying on VPNs.

Shop floor devices using SINEC Secure Connect remain protected from unauthorized external access while maintaining the necessary operational connectivity. This allows industrial companies to realize secure, flexible, and future-proof OT networking. …

Source and more information:

https://www.helpnetsecurity.com/2025/10/01/siemens-sinec-secure-connect/

NIST Publishes Guide for Protecting ICS Against USB-Borne Threats

NIST has published a new guide designed to help organizations reduce cybersecurity risks associated with the use of removable media devices in operational technology (OT) environments.

NIST Special Publication (SP) 1334 was authored by the National Cybersecurity Center of Excellence (NCCoE) and it focuses on the use of USB flash drives, but also mentions other types of removable media such as external hard drives and CD/DVD drives.

USB flash drives are often used in OT environments to conduct firmware updates or to retrieve data for diagnostics purposes, but such devices are also often a source of malware infections. …

Source and more information:

https://www.securityweek.com/nist-publishes-guide-for-protecting-ics-against-usb-borne-threats/

The Phantom Slice (How Silent Protocol Exploits In 5g Are Creating A Ticking Time Bomb In Critical Infrastructure)

Imagine an energy utility's grid stabilization system, operating on a dedicated, "secure" 5G network slice, experiencing a catastrophic failure. The root cause is not a breach of the operational technology (OT) network itself, but a single, malformed data packet originating from a compromised smart streetlamp on a completely separate municipal services slice. This is not a future scenario; it is the present danger. The software-defined nature of 5G, specifically network slicing, has created a new, insidious attack surface. Threat actors are no longer attacking the perimeter of a slice but are exploiting the foundational protocols of the shared 5G core, turning the promise of isolation into a dangerous illusion. …

Source and more information:

CDM-CYBER-DEFENSE-eMAGAZINE-October-2025.pdf

Many Attacks Aimed at EU Targeted OT, Says Cybersecurity Agency

The European Union’s cybersecurity agency ENISA has published its 2025 Threat Landscape report, which shows that a significant percentage of the attacks aimed at the EU over the past year targeted operational technology (OT) systems.

The report is based on the analysis of nearly 4,900 cybersecurity incidents recorded between July 2024 and June 2025. This includes publicly reported incidents, as well as attacks reported to ENISA by EU countries and members of an ENISA information sharing program. …

Source and more information:

https://www.securityweek.com/many-attacks-aimed-at-eu-targeted-ot-says-cybersecurity-agency/

Researchers track Cavalry Werewolf custom malware attacks on Russian government, industrial networks

New research from BI.ZONE Threat Intelligence tracked Cavalry Werewolf activity between May and August 2025. The group primarily targeted Russian state agencies, along with enterprises in the energy, mining, and manufacturing sectors. These adversaries impersonate government officials and deploy custom-built malware to carry out their operations. To gain initial access, Cavalry Werewolf sent spear-phishing emails disguised as official correspondence from Kyrgyz government officials. Each email contained a RAR archive that deployed either FoalShell, a reverse shell, or StallionRAT, a remote access trojan controlled via Telegram, allowing the attackers to maintain stealthy command-and-control over compromised systems. …

Source and more information:

https://industrialcyber.co/ransomware/researchers-track-cavalry-werewolf-custom-malware-attacks-on-russian-government-industrial-networks/

Radiflow360 unifies OT risk, compliance, and response

Radiflow has launched the new Radiflow360, a unified, AI-enhanced OT cybersecurity platform that delivers visibility, risk management and streamlined incident response for mid-sized industrial enterprises.

Radiflow360 now enables mid-sized industrial operators to gain visibility and control over their OT networks and risks, and is supported by an AI analyst assistant that speeds up assessments and prioritizes threats. …

Source and more information:

https://www.helpnetsecurity.com/2025/10/08/radiflow-radiflow360/

The five-minute guide to OT cyber resilience

In this Help Net Security video, Rob Demain, CEO of e2e-assure, explains the essentials of OT cybersecurity resilience. He discusses the importance of understanding remote access points, supply chain connections, and the need for specialized sensors to monitor OT networks that differ from traditional IT systems.

Demain emphasizes knowing what normal behavior looks like, linking changes to management systems, and maintaining accurate asset inventories. Demain concludes that availability is the top priority in OT, and resilience means keeping systems safe and operational even under cyberattack. …

Source and the video:

https://www.helpnetsecurity.com/2025/10/13/ot-cybersecurity-resilience-video/

A safer way to break industrial systems (on purpose)

Cybersecurity teams often struggle to test defenses for industrial control systems without risking disruption. A group of researchers from Curtin University has developed a way to make that easier. Their work introduces a container-based framework that lets researchers and practitioners simulate real control system environments and run cyberattacks on them safely.

Industrial control systems (ICS) run everything from water treatment plants to power grids. Because they manage physical processes, testing them directly can be risky. Many organizations either use outdated datasets or rely on narrow simulations that model only one system type. That limitation has slowed progress in building and validating intrusion detection systems for industrial networks. …

Source and more information:

https://www.helpnetsecurity.com/2025/10/15/industrial-control-system-simulation-cybersecurity/

The Fight Against Ransomware Heats Up on the Factory Floor

Ransomware gangs continue to set their sights on the manufacturing industry, but companies are taking steps to protect themselves, starting with implementing timely patch management protocols.

Ransomware groups come and go, but one constant is that manufacturing remains a top target.

The ransomware landscape is ever-evolving. New groups emerge and old ones dismantle or rebrand. Ransomware-as-a-service (RaaS) launched and lowered the barrier to entry. Even the name "ransomware" doesn't always apply now, as some groups rely solely on data extortion threats over encryption to pressure victims into paying. And, of course, attackers are increasingly using artificial intelligence (AI). …

Source and more information:

https://www.darkreading.com/ics-ot-security/ransomware-manufacturing-an-escalating-battle

As industrial systems modernize, adaptive OT cybersecurity replaces patchwork defense

The OT (operational technology) cybersecurity landscape is constantly evolving to adaptive OT cybersecurity, which traditional defenses have often overlooked. Latest OT security features use AI-powered anomaly recognition, sophisticated network micro-segmentation, and flexible encryption to secure the connection of the industrial systems more efficiently. These advances form the foundation of adaptive OT cybersecurity, closing invisible gaps without operational disruption, thus allowing continuous verification and adaptive defenses that are specifically customized for legacy environments that were not initially developed for modern cybersecurity. …

Source and more information:

https://industrialcyber.co/features/as-industrial-systems-modernize-ot-cybersecurity-moves-from-patchwork-defense-to-continuous-adaptive-protection/

New Microchip Tech Protects Vehicles from Laser Attacks

Researchers are proposing that microchip manufacturers adopt a new multi-layered, insulating design to protect them against cyber-physical attacks, primarily from lasers.

On Monday, members of the French Alternative Energies and Atomic Energy Commission (CEA) and Soitec, a semiconductor manufacturing company, released a report advocating for a new kind of microchip technology designed to strengthen automotive cybersecurity. It's called "Fully Depleted Silicon-on-Insulator" (FD-SOI), and it obstructs cyber-physical attacks against chips, making already elaborate and costly attack scenarios even more unrealistic than they might already seem. …

Source and more information:

https://www.darkreading.com/ics-ot-security/microchip-tech-vehicles-laser-attacks

Fuji Electric HMI Configurator Flaws Expose Industrial Organizations to Hacking

Several vulnerabilities patched recently by Fuji Electric in its V-SFT product could be exploited by threat actors to gain access to the systems of industrial organizations.

Fuji Electric (Hakko Electronic) V-SFT is a configuration and development software for human-machine interfaces (HMIs). Organizations in the manufacturing and other industrial sectors use it to create and manage user interfaces for Fuji Electric’s Monitouch series HMIs, which are widely used around the world.

Cybersecurity researcher Michael Heinzl discovered that V-SFT is affected by several vulnerabilities, including ones that can lead to information disclosure or arbitrary code execution on the system running the software. …

Source and more information:

https://www.securityweek.com/fuji-electric-hmi-configurator-flaws-expose-industrial-organizations-to-hacking/

Electronic Warfare Puts Commercial GPS Users on Notice

Localized jamming and spoofing of global navigation satellite systems (GNSS) continues to be a hallmark of conflicts across the globe, with the digital signal attacks impacting air travel and transport and maritime shipping. And now, the denial-of-service issue seems to be affecting everyday organizations in other verticals, too. …

Source and more information:

https://www.darkreading.com/cybersecurity-operations/electronic-warfare-commercial-gps-users-notice

Forescout warns TP-Link router vulnerabilities could expose industrial systems, provides mitigations

New data from Forescout Technologies reveals two critical vulnerabilities in TP-Link Omada and Festa VPN routers, which are deployed across connected devices ranging from solar inverters to programmable logic controllers. CVE-2025-7850 allows OS command injection via WireGuard VPN settings, while CVE-2025-7851 enables unauthorized root access through residual debug code. A partial fix for CVE-2024-21827 left debug functionality exposed, opening new attack vectors.

CVE-2025-7850 can be exploited remotely in certain setups without credentials, as protocol analysis indicates scenarios beyond the initial local exploitation. Additional critical flaws were identified across TP-Link devices, with a full disclosure expected after patches are released in the first quarter of next year. Using the root foothold, Forescout identified multiple additional issues affecting other TP-Link models; those issues are in coordinated disclosure, after which it will publish full technical details. …

Source and more information:

https://industrialcyber.co/reports/forescout-warns-tp-link-router-vulnerabilities-could-expose-industrial-systems-provides-mitigations/

CSIS: USCG poised for ‘generational change’ in maritime cybersecurity with new tools, $25B funding

Analysis from the Center for Strategic and International Studies (CSIS) identifies a chance for generational change in safeguarding the maritime cyber domain and strengthening the U.S. Coast Guard’s cyber workforce. Recent regulatory, legislative, and policy developments have given the Coast Guard new cybersecurity tools and expanded authorities to protect the marine transportation system from cyber threats. This comes as the agency's historic budget challenges have eased. With nearly $25 billion in funding from the One Big Beautiful Bill Act, the Coast Guard now finds itself in the rare position of having resources and momentum on its side. …

Source and more information:

https://industrialcyber.co/transport/csis-uscg-poised-for-generational-change-in-maritime-cybersecurity-with-new-tools-25b-funding/

Canada's Cyber Centre urges action as Internet-accessible ICS face growing cyber threats from hacktivists

The Canadian Centre for Cyber Security issued an alert warning chief information security officers (CISOs) and decision-makers about Internet-accessible ICS (industrial control systems) being targeted by hacktivists. The alert aims to raise awareness of this emerging cyber threat, outline potential impacts on critical systems, and offer detection and mitigation guidance. The Cyber Centre also offers direct assistance to organizations seeking further support on the alert's findings. …

Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/canadas-cyber-centre-urges-action-as-internet-accessible-ics-face-growing-cyber-threats-from-hacktivists/

Industrial Giants Schneider Electric and Emerson Named as Victims of Oracle Hack

Industrial giants Schneider Electric and Emerson have been named by cybercriminals as victims of the recent campaign targeting Oracle E-Business Suite (EBS) instances.

Threat actors, presumably a cluster of the FIN11 profit-driven threat group, have exploited Oracle EBS vulnerabilities to steal data from dozens of organizations, including major companies.

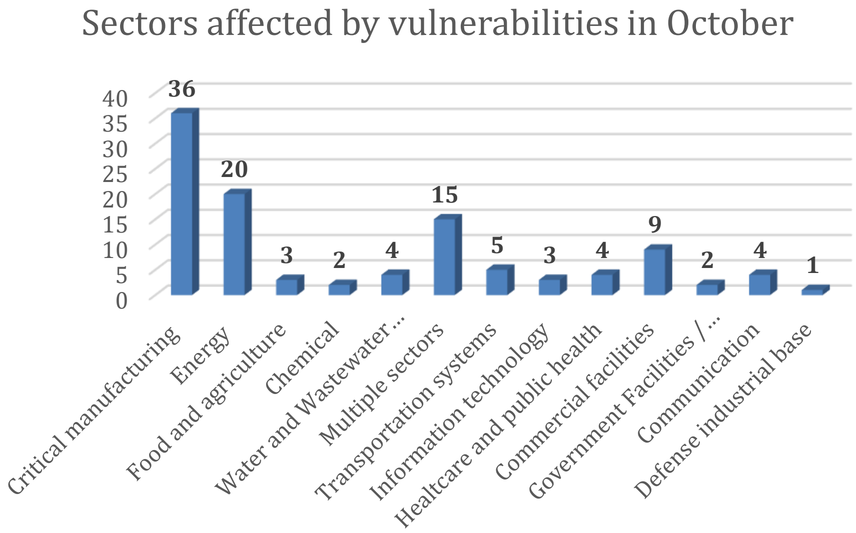
The hackers have started naming alleged victims on the leak website set up for the Cl0p ransomware, and in some cases they have started releasing data that allegedly originates from the targeted companies. …

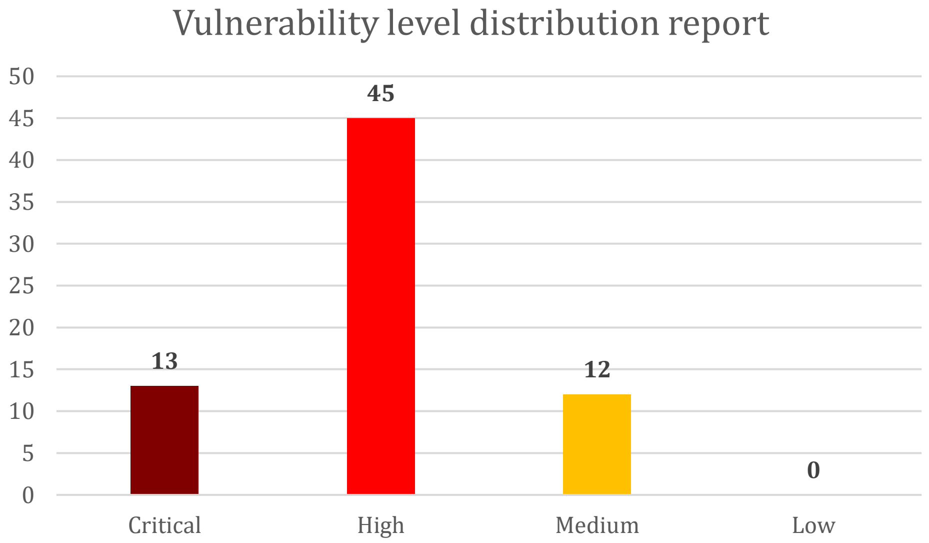
Source and more information:

https://www.securityweek.com/industrial-giants-schneider-electric-and-emerson-named-as-victims-of-oracle-hack/

ICS vulnerabilities

In October 2025, 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-25-303-01: **International Standards Organization ISO 15118-2**

High level vulnerability: Improper Restriction of Communication Channel to Intended Endpoints.

International Standards Organization ISO 15118-2 | CISA

ICSA-25-303-02: **Hitachi Energy TropOS**

High level vulnerabilities: OS Command Injection, Improper Privilege Management.

Hitachi Energy TropOS | CISA

ICSA-25-301-01: **Schneider Electric EcoStruxure**

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

Schneider Electric EcoStruxure | CISA

ICSMA-25-301-01: **Vertikal Systems Hospital Manager Backend Services**

High level vulnerabilities: Exposure of Sensitive System Information to an Unauthorized Control Sphere, Generation of Error Message Containing Sensitive Information.

Vertikal Systems Hospital Manager Backend Services | CISA

ICSA-24-352-04: **Schneider Electric Modicon (Update B)**

Critical level vulnerability: Improper Input Validation.

Schneider Electric Modicon (Update B) | CISA

ICSA-25-296-01: **AutomationDirect Productivity Suite**

Critical level vulnerabilities: Relative Path Traversal, Weak Password Recovery Mechanism for Forgotten Password, Incorrect Permission Assignment for Critical Resource, Binding to an Unrestricted IP Address.

AutomationDirect Productivity Suite | CISA

ICSA-25-296-02: **ASKI Energy ALS-Mini-S8 and ALS-Mini-S4**

Critical level vulnerability: Missing Authentication for Critical Function.

ASKI Energy ALS-Mini-S8 and ALS-Mini-S4 | CISA

ICSA-25-296-03: **Veeder-Root TLS4B Automatic Tank Gauge System**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in a Command ('Command Injection'), Integer Overflow or Wraparound.

Veeder-Root TLS4B Automatic Tank Gauge System | CISA

ICSA-25-296-04: **Delta Electronics ASDA-Soft**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics ASDA-Soft | CISA

ICSMA-25-296-01: **NIHON KOHDEN Central Monitor CNS-6201**

High level vulnerability: NULL Pointer Dereference.

NIHON KOHDEN Central Monitor CNS-6201 | CISA

ICSA-25-037-02: **Schneider Electric EcoStruxure (Update C)**

High level vulnerability: Uncontrolled Search Path Element.

Schneider Electric EcoStruxure (Update C) | CISA

ICSA-24-116-02: **Hitachi Energy MACH SCM (Update A)**

High level vulnerabilities: Improper Control of Generation of Code, Improper Neutralization of Directives in Dynamically Evaluated Code.

Hitachi Energy MACH SCM (Update A) | CISA

ICSA-25-259-01: **Schneider Electric Altivar products, ATVdPAC module, ILC992 InterLink Converter (Update A)**

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

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

ICSA-25-294-01: **Rockwell Automation 1783-NATR**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Cross-Site Request Forgery (CSRF).

Rockwell Automation 1783-NATR | CISA

ICSA-25-294-02: **Rockwell Automation Compact GuardLogix 5370**

High level vulnerability: Uncaught Exception.

Rockwell Automation Compact GuardLogix 5370 | CISA

ICSA-25-294-03: **Siemens SIMATIC S7-1200 CPU V1/V2 Devices**

High level vulnerabilities: Improper Input Validation, Authentication Bypass by Capture-replay.

Siemens SIMATIC S7-1200 CPU V1/V2 Devices | CISA

ICSA-25-294-04: **Siemens RUGGEDCOM ROS Devices**

High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Improper Handling of Exceptional Conditions, Protection Mechanism Failure.

Siemens RUGGEDCOM ROS Devices | CISA

ICSA-25-294-05: **CloudEdge Online Cameras and App**

High level vulnerability: Use of Hard-coded Credentials.

CloudEdge Online Cameras and App | CISA

ICSA-25-294-06: **Raisecomm RAX701-GC Series**

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

Raisecomm RAX701-GC Series | CISA

ICSMA-25-294-:01 **Oxford Nanopore Technologies MinKNOW**

High level vulnerabilities: Missing Authentication for Critical Function, Insufficiently Protected Credentials, Improper Check for Unusual or Exceptional Conditions.

Oxford Nanopore Technologies MinKNOW | CISA

ICSA-25-035-07: **Schneider Electric Pro-Face GP-Pro EX and Remote HMI (Update A)** **Medium** level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Schneider Electric Pro-face GP-Pro EX and Remote HMI (Update A) | CISA

ICSA-24-354-07: **Schneider Electric Modicon Controllers (Update A)**

Medium level vulnerability: Cross-site Scripting.

Schneider Electric Modicon Controllers (Update A) | CISA

ICSA-25-140-08: **Schneider Electric Modicon Controllers (Update B)**

High level vulnerability: Externally Controlled Reference to a Resource in Another Sphere.

Schneider Electric Modicon Controllers (Update B) | CISA

ICSA-25-289-01: **Rockwell Automation FactoryTalk View Machine Edition and PanelView Plus 7**

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

Rockwell Automation FactoryTalk View Machine Edition and PanelView Plus 7 | CISA

ICSA-25-289-02: **Rockwell Automation FactoryTalk Linx**

High level vulnerability: Privilege Chaining.

Rockwell Automation FactoryTalk Linx | CISA

ICSA-25-289-03: **Rockwell Automation FactoryTalk ViewPoint**

High level vulnerability: Improper Restriction of XML External Entity Reference.

Rockwell Automation FactoryTalk ViewPoint | CISA

ICSA-25-289-04: **Rockwell Automation ArmorStart AOP**

High level vulnerability: Uncaught Exception.

Rockwell Automation ArmorStart AOP | CISA

ICSA-25-289-05: **Siemens Solid Edge**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read.

Siemens Solid Edge | CISA

ICSA-25-289-06: **Siemens SiPass Integrated**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Cross-site Scripting, Authorization Bypass Through User-Controlled Key, Storing Passwords in a Recoverable Format.

Siemens SiPass Integrated | CISA

ICSA-25-289-07: **Siemens SIMATIC ET 200SP Communication Processors**

Critical level vulnerability: Missing Authentication for Critical Function.

Siemens SIMATIC ET 200SP Communication Processors | CISA

ICSA-25-289-08: **Siemens SINEC NMS**

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

Siemens SINEC NMS | CISA

ICSA-25-289-09: **Siemens TeleControl Server Basic**

Critical level vulnerability: Missing Authentication for Critical Function.

Siemens TeleControl Server Basic | CISA

ICSA-25-289-10: **Siemens HyperLynx and Industrial Edge App Publisher**

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

Siemens HyperLynx and Industrial Edge App Publisher | CISA

ICSA-25-289-11: **Hitachi Energy MACH GWS**

High level vulnerabilities: Incorrect Default Permissions, Improper Validation of Integrity Check Value, Improper Certificate Validation.

Hitachi Energy MACH GWS | CISA

ICSA-25-224-03: **Schneider Electric EcoStruxure (Update A)**

High level vulnerabilities: Deserialization of Untrusted Data, Server-Side Request Forgery (SSRF), Path Traversal.

Schneider Electric EcoStruxure (Update A) | CISA

ICSA-24-121-01: **Delta Electronics CNCSoft-G2 DOPSoft (Update A)**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics CNCSoft-G2 DOPSoft (Update A) | CISA

ICSA-25-287-01: **Rockwell Automation 1715 EtherNet/IP Comms Module**

High level vulnerabilities: Allocation of Resources Without Limits or Throttling, Out-of-bounds Write.

Rockwell Automation 1715 EtherNet/IP Comms Module | CISA

SSA-978177: **Vulnerability in Nozomi Guardian/CMC on RUGGEDCOM APE1808 Devices (Update 1.1.)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Execution with Unnecessary Privileges, Incorrect Authorization, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incorrect Authorization, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

SSA-978177

SSA-876787: **Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs (Update 1.9.)**

Medium level vulnerability: URL Redirection to Untrusted Site ('Open Redirect').

SSA-876787

SSA-722410: **Multiple Vulnerabilities in User Management Component (UMC) (Update 1.1.)**

Critical level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read.

SSA-722410

SSA-693808: **Deserialization Vulnerability in Siemens Engineering Platforms (Update 1.1.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-693808

SSA-614723: **Denial of Service Vulnerabilities in User Management Component (UMC) (Update 1.2.)**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.

SSA-614723

SSA-513708: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices (Update 1.2.)**

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.

SSA-513708

SSA-493396: **Deserialization Vulnerability in Siemens Engineering Platforms (Update 1.1.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-493396

SSA-373591: **Buffer Overflow Vulnerability in RUGGEDCOM ROS Devices (Update 1.2.)** **High** level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

SSA-373591

SSA-367714: **Improper Integrity Check of Firmware Updates in SiPass integrated AC5102 / ACC-G2 and ACC-AP (Update 1.1.)**

High level vulnerability: Improper Verification of Cryptographic Signature.

SSA-367714

SSA-282044: **DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery (Update 1.2.)**

High level vulnerability: Uncontrolled Search Path Element.

SSA-282044

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1 (Update 2.0.)**

Medium level vulnerabilities: Multiple.

SSA-265688

SSA-186293: **XML External Entity (XXE) Injection Vulnerability in SIMOTION SCOUT, SIMOTION SCOUT TIA and SINAMICS STARTER (Update 1.1.)**

Medium level vulnerability: Improper Restriction of XML External Entity Reference.

SSA-186293

SSA-083019: **Multiple Vulnerabilities in RUGGEDCOM ROS Devices (Update 1.1.)**

High level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Improper Handling of Exceptional Conditions, Protection Mechanism Failure.

SSA-083019

SSA-054046: **Unauthenticated Information Disclosure in Web Server of SIMATIC S7-1500 CPUs (Update 1.7.)**

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

SSA-054046

SSA-039007: **Heap-based Buffer Overflow Vulnerability in User Management Component (UMC)** **(Update 1.6.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-039007

ICSA-25-282-01: **Hitachi Energy Asset Suite**

Medium level vulnerability: Improper Output Neutralization for Logs.

Hitachi Energy Asset Suite | CISA

ICSA-25-282-02: **Rockwell Automation Lifecycle Services with Cisco**

Medium level vulnerability: Stack-based Buffer Overflow.

Rockwell Automation Lifecycle Services with Cisco | CISA

ICSA-25-282-03: **Rockwell Automation Stratix**

Medium level vulnerability: Stack-based Buffer Overflow.

Rockwell Automation Stratix | CISA

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

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

Mitsubishi Electric Multiple FA Products (Update A) | CISA

ICSA-25-280-01: **Delta Electronics DIAScreen**

Medium level vulnerability: Out-of-bounds Write.

Delta Electronics DIAScreen | CISA

ICSA-25-226-31: **Rockwell Automation 1756-EN4TR, 1756-EN4TRXT** **(Update B)**

High level vulnerabilities: Improper Input Validation, Improper Handling of Exceptional Conditions.

Rockwell Automation 1756-EN4TR, 1756-EN4TRXT (Update B) | CISA

ICSA-25-275-01: **Raise3D Pro2 Series 3D Printers**

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

Raise3D Pro2 Series 3D Printers | CISA

ICSA-25-275-02: **Hitachi Energy MSM Product**

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

Hitachi Energy MSM Product | CISA

ICSA-25-273-01: **MegaSys Enterprises Telenium Online Web Application**

Critical level vulnerability: OS Command Injection.

MegaSys Enterprises Telenium Online Web Application | CISA

ICSA-25-273-02: **Festo SBRD-Q/SBOC-Q/SBOI-Q**

High level vulnerabilities: Incorrect Conversion between Numeric Types, Out-of-bounds Read, Reachable Assertion.

Festo SBRD-Q/SBOC-Q/SBOI-Q | CISA

ICSA-25-273-03: **Festo CPX-CEC-C1 and CPX-CMXX**

High level vulnerability: Improper Privilege Management.

Festo CPX-CEC-C1 and CPX-CMXX | CISA

ICSA-25-273-04: **Festo Controller CECC-S,-LK,-D Family Firmware**

Critical level vulnerabilities: Exposure of Resource to Wrong Sphere, Untrusted Pointer Dereference, NULL Pointer Dereference, Files or Directories Accessible to External Parties, Out-of-bounds Write, Improper Privilege Management, Incorrect Permission Assignment for Critical Resource, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Missing Release of Memory after Effective Lifetime, Improper Handling of Exceptional Conditions, Use of a Broken or Risky Cryptographic Algorithm, Weak Password Recovery Mechanism for Forgotten Password, Use of Password Hash With Insufficient Computational Effort, Improper Access Control, Allocation of Resources Without Limits or Throttling, Improper Input Validation, Buffer Over-read, Use of Insufficiently Random Values, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Uncontrolled Recursion, Missing Encryption of Sensitive Data, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Festo Controller CECC-S,-LK,-D Family Firmware | CISA

ICSA-25-273-05: **OpenPLC_V3**

Medium level vulnerabilities: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior.

OpenPLC_V3 | CISA

ICSA-25-273-06: **National Instruments Circuit Design Suite**

High level vulnerabilities: Type Confusion, Out-of-bounds Read.

National Instruments Circuit Design Suite | CISA

ICSA-25-273-07: **LG Innotek Camera Multiple Models**

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

LG Innotek Camera Multiple Models | CISA

ICSA-25-063-02: **Keysight Ixia Vision Product Family (Update A)**

High level vulnerabilities: Path Traversal, Improper Restriction of XML External Entity Reference, Use of Hard-coded Cryptographic Key.

Keysight Ixia Vision Product Family (Update A) | CISA

ICSA-22-298-02: **HEIDENHAIN Controller TNC (Update A)**

Critical level vulnerability: Improper Authentication.

HEIDENHAIN Controller TNC (Update A) | CISA

ICSA-25-226-26: **Rockwell Automation FLEX 5000 I/O (Update A)**

High level vulnerability: Improper Input Validation.

Rockwell Automation FLEX 5000 I/O (Update A) | CISA

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

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.

ICS alerts

CISA has published alerts in 2025 October:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2014-6278 GNU Bash OS Command Injection Vulnerability;
CVE-2015-7755 Juniper ScreenOS Improper Authentication Vulnerability;
CVE-2017-1000353 Jenkins Remote Code Execution Vulnerability;
CVE-2025-4008 Smartbedded Meteobridge Command Injection Vulnerability;
CVE-2025-21043 Samsung Mobile Devices Out-of-Bounds Write Vulnerability;
CVE-2010-3765 Mozilla Multiple Products Remote Code Execution Vulnerability;
CVE-2010-3962 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability;
CVE-2011-3402 Microsoft Windows Remote Code Execution Vulnerability;
CVE-2013-3918 Microsoft Windows Out-of-Bounds Write Vulnerability;
CVE-2021-22555 Linux Kernel Heap Out-of-Bounds Write Vulnerability;
CVE-2021-43226 Microsoft Windows Privilege Escalation Vulnerability;
CVE-2025-61882 Oracle E-Business Suite Unspecified Vulnerability;
CVE-2025-27915 Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability;
CVE-2021-43798 Grafana Path Traversal Vulnerability;
CVE-2016-7836 SKYSEA Client View Improper Authentication Vulnerability;
CVE-2025-6264 Rapid7 Velociraptor Incorrect Default Permissions Vulnerability;
CVE-2025-24990 Microsoft Windows Untrusted Pointer Dereference Vulnerability;
CVE-2025-47827 IGEL OS Use of a Key Past its Expiration Date Vulnerability;
CVE-2025-59230 Microsoft Windows Improper Access Control Vulnerability;
CVE-2025-54253 Adobe Experience Manager Forms Code Execution Vulnerability;
CVE-2022-48503 Apple Multiple Products Unspecified Vulnerability;
CVE-2025-2746 Kentico Xperience Staging Sync Server Digest Password Authentication Bypass Vulnerability;
CVE-2025-2747 Kentico Xperience Staging Sync Server None Password Type Authentication Bypass Vulnerability;
CVE-2025-33073 Microsoft Windows SMB Client Improper Access Control Vulnerability;
CVE-2025-61884 Oracle E-Business Suite Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2025-61932 Motex LANSCOPE Endpoint Manager Improper Verification of Source of a Communication Channel Vulnerability;
CVE-2025-54236 Adobe Commerce and Magento Improper Input Validation Vulnerability;
CVE-2025-59287 Microsoft Windows Server Update Service (WSUS) Deserialization of Untrusted Data Vulnerability;
CVE-2025-6204 Dassault Systèmes DELMIA Apriso Code Injection Vulnerability;
CVE-2025-6205 Dassault Systèmes DELMIA Apriso Missing Authorization Vulnerability;

CVE-2025-24893 XWiki Platform Eval Injection Vulnerability;
CVE-2025-41244 Broadcom VMware Aria Operations and VMware Tools Privilege Defined with Unsafe Actions Vulnerability;
Links and more information:
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Seven 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 Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds 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 Directs Federal Agencies to Mitigate Vulnerabilities in F5 Devices
CISA issued Emergency Directive ED 26-01: Mitigate Vulnerabilities in F5 Devices to direct Federal Civilian Executive Branch agencies to inventory F5 BIG-IP products, evaluate if the networked management interfaces are accessible from the public internet, and apply newly released updates from F5.
Links and more information:
CISA Directs Federal Agencies to Mitigate Vulnerabilities in F5 Devices | CISA

Microsoft Releases Out-of-Band Security Update to Mitigate Windows Server Update Service Vulnerability, CVE-2025-59287
Microsoft released an update to address a critical remote code execution vulnerability impacting Windows Server Update Service (WSUS) in Windows Server (2012, 2016, 2019, 2022, and 2025), CVE-2025-59287, that a prior update did not fully mitigate.
Links and more information:
Microsoft Releases Out-of-Band Security Update to Mitigate Windows Server Update Service Vulnerability, CVE-2025-59287 | CISA

New Guidance Released on Microsoft Exchange Server Security Best Practices
CISA, in partnership with the National Security Agency and international cybersecurity partners, released Microsoft Exchange Server Security Best Practices, a guide to help network defenders harden on-premises Exchange servers against exploitation by malicious actors.
Links and more information:
New Guidance Released on Microsoft Exchange Server Security Best Practices | CISA

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in November 2025:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Industrial Control Systems Cybersecurity (Virtual)(ICS300)
- Industrial Control Systems Evaluation (Virtual)(401V)
- ICS Cybersecurity & RED-BLUE Exercise (In-Person)(ICS301)
- Industrial Control Systems Evaluation (In-Person)(401L)
- Introduction to Control Systems Cybersecurity (In-Person)(101)
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- ICS/SCADA Cyber Security
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

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

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

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

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

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

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

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

https://www.udemy.com/course/ics-cybersecurity/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

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

- OT Railway Cybersecurity (OTCS)

https://informaconnect.com/ot-railway-cybersecurity-otcs/

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

https://opswatacademy.com/courses/ot-security-expert

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

https://www.yokogawa.com/eu/solutions/products-and-services/trainings-und-workshops/kompetenztrainings/ctr-008-ot-security-awareness-e-learning-course/

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

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

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/