2025 April, 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 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.

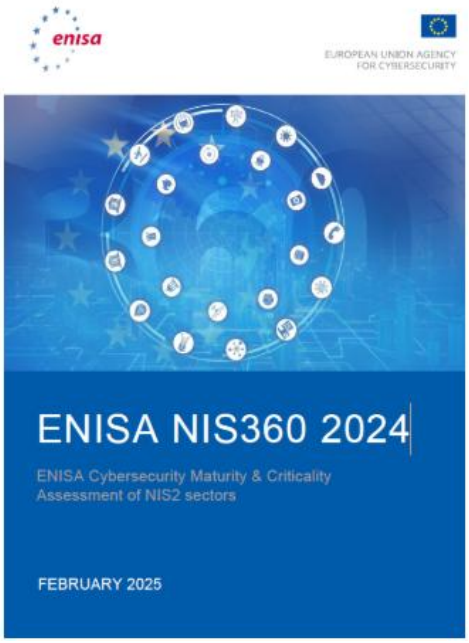
Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/

ICS good practices, recommendations

ENISA NIS360 2024

The NIS360 is a new ENISA product that assesses the maturity and criticality of sectors of high criticality under the NIS2 Directive, providing both a comparative overview and a more in-depth analysis of each sector. The NIS360 is designed to assist Member States and national authorities in identifying gaps and prioritising resources. The analysis is based on data from national authorities with a horizontal or sectorial mandate, data from companies within the in-scope sectors, and insights from EU-level sources such as Eurostat.

The assessment takes the following sectors into account: Energy, Transport, Finance, Health, Drinking and Wastewater, Digital Infrastructure, ICT Service Management, Public Administration, Space.



Organizations belonging to a given sector should read the relevant sections.

Source and more detailed information available on the following link:

https://www.enisa.europa.eu/publications/enisa-nis360-2024

ICS trainings, education

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

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

TechNet Cyber 2025

Join the conference in Baltimore, Maryland for this three-day event and interact with IT & OT professionals, hear from experts and develop solutions to ensure technology can connect people to information.

This year's theme is Empowering the Warfighter: Innovate, Integrate, Dominate. Connect with us at the event and be a part of the conversation led by U.S. Cyber Command, DISA, the DoD CIO, and numerous industry and academia partners to deliver solutions for this enduring, no-fail mission.

Baltimore, Maryland, USA; 6th - 8th May 2025

More details can be found on the following website:

https://www.industrialdefender.com/events/technet-cyber-2025

8th IEEE Conference on Industrial Cyber-Physical Systems

Continuing with the success of the past ICPS-Editions held in Russia (2018), Taiwan (2019), Finland (2020), Canada (2021), the UK (2022), China (2023), and the USA (2024), ICPS 2025, under the motto "The Ongoing Digital Transformation", aims to provide an international platform for cutting-edge research and professional interactions for the development of ICPS. Industry experts, researchers, and academics will share ideas and experiences surrounding frontier technologies, breakthroughs, innovative solutions, research and innovation results, as well as initiatives related to ICPS, AI-assisted Digital Transformation, and their applications. The conference program will feature a rich program, including research and innovation papers, as well as special sessions, tutorials, exhibitions, and an industry forum with thematic dedicated industry talks.

Emden, Germany; 12th – 15th May 2025

More details can be found on the following website:

https://icps2025.ieee-ies.org/

IoT / OT Security Conference

OT systems are connected to the IT in the company network and supply data from sensors, for example. However, older production machines in particular are often not designed for remote access. This can compromise cybersecurity and favour cyberattacks. Management has a duty to view cybersecurity as a corporate responsibility rather than a necessary evil.

Many organisations in critical infrastructures and industrial companies underestimate the dangers that lurk here. Attacks on these sectors are on the rise. Today, it is important to protect existing infrastructures in the best possible way. For new devices, it will be crucial to consider security right from the design stage. This can also create competitive advantages.

The IoT / OT Security Conference will show you where dangers lurk and what solutions are available.

Cham, Switzerland; 20th May 2025

More details can be found on the following website:

https://www.swissbit.com/en/company/events/iot-ot-security-conference-2025-2/

Industrial Cyber Show

Industrial Cyber Show debuts in the heart of Las Vegas, merging the unrivaled expertise of the globally renowned CS4CA and ManuSec summits. This exclusive two-day event will unite 150+ leaders tasked with securing the IT-OT convergence, creating a powerful arena for sharing actionable cybersecurity insights, breakthrough strategies, and making high-impact connections.

Designed for active learning and collaboration, the summit features an action-packed agenda with deep-dive panel discussions, immersive workshops, and interactive networking sessions. This is your chance to forge strategic partnerships with top cybersecurity executives from industries like: Manufacturing, Oil & Gas, Energy, Mining, Transportation, Maritime, Healthcare & Life Sciences, Semiconductors, Data Centers… And to lead the discussions shaping the OT security landscape in 2025 and beyond.

Las Vegas, Nevada, USA; 20th – 21st May 2025

More details can be found on the following website:

https://industrialcybershow.cs4ca.com/

ICS incidents

Cyber Hackers Claim To Have Disrupted Communication Networks of 116 Iranian Ships

A significant cyberattack, claimed by the hacker group Lab Dookhtegan, has disrupted communication systems aboard 116 Iranian vessels belonging to two major state-affiliated shipping companies — the National Iranian Tanker Company (NITC) and the Islamic Republic of Iran Shipping Lines (IRISL). The group announced on Telegram that the attack aimed to expose and disrupt the companies' alleged support for illegal activities, including the supply of munitions to the Houthi rebels.

The timing of the attack appears to align with ongoing U.S. military operations targeting the Houthis, suggesting a coordinated strategic intent. The hackers stated that the vessels' internal and external communication systems were severely affected, impeding coordination between ships, with ports, and with other stakeholders. The attack reportedly left vessels without reliable GPS or standard maritime communications, with the potential restoration timeline spanning several weeks.

Crucially, maritime cybersecurity experts, including Cyndome, emphasized the broader implications of the attack for both Information Technology (IT) and Operational Technology (OT) systems. According to Cyndome, shipboard communication devices are not only critical for navigation and coordination but can also serve as entry points for deeper compromises. If attackers gain access through these channels, they may pivot into OT environments, potentially affecting physical systems such as propulsion, ballast control, or cargo handling.

The nature of the attack — involving simultaneous targeting of over 100 vessels — indicates a high level of planning, automation, and adversarial sophistication. The United Kingdom Maritime Trade Operations Centre corroborated reports of GPS interference in the Strait of Hormuz, further validating the scale and potential physical safety implications of the incident. At the time of reporting, neither Iranian government representatives nor the affected shipping companies have publicly acknowledged the cyberattack, leaving the scope and damage largely unconfirmed from official sources. Nonetheless, this incident serves as a stark reminder of the growing threat to maritime OT systems and the need for comprehensive cyber resilience strategies across critical infrastructure sectors.

The source is available on the following link:

https://www.marineinsight.com/shipping-news/cyber-hackers-claim-to-have-disrupted-communication-networks-of-116-iranian-ships/

Book recommendation

INDUSTRIAL CYBERSECURITY: A Practical Approach To Operational Technology Protection

INDUSTRIAL CYBERSECURITY: A Practical Approach to Operational Technology Protection is carefully designed to guide you through everything you need to know about Operational technology and its Cybersecurity aspect as per NIST standards, from the basics to the most advanced concepts. Unlock the Secrets to Securing Operational Technology!

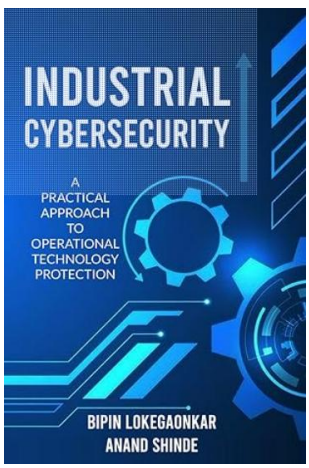
Starting with the fundamental principles of OT, this comprehensive guide delves into critical aspects such as industrial control systems, network security, and, most importantly, how to implement security controls in accordance with the National Institute of Standards and Technology (NIST) SP 800-82 – Rev 3 standard. This standard offers comprehensive guidelines for securing ICS and other critical infrastructure components against cyber threats, helping organizations fortify their OT environments against a rapidly evolving threat landscape.

Author/Editor: Anand Shinde (Autor), Bipin Lokegaonkar (Autor)

Year of issue: 2024

The book is available at the following link:

https://www.amazon.de/INDUSTRIAL-CYBERSECURITY-Operational-Technology-Protection/dp/191686502X/ref=asc_df_191686502X?mcid=661b815cb8e23bf79c8ba7498ad1e3d9&th=1&psc=1&hvocijid=11880887634635869328-191686502X-&hvexpln=75&tag=googshopde-21&linkCode=df0&hvadid=696184104678&hvpos=&hvnetw=g&hvrand=11880887634635869328&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9195996&hvtargid=pla-2281435175978&psc=1&gad_source=1



ICS security news selection

Security Tech That Can Make a Difference During an Attack

When the FBI contacted Massachusetts-based Littleton Electric Light and Water Departments (LELWD) about Volt Typhoon, the small public utility was unaware that the Chinese attack group had been in the company's network for more than 300 days.

While the utility had security controls protecting the perimeter, its security technology and policy had some gaps. A more rigorous update strategy for its network and security appliances would have prevented the initial compromise. In addition, monitoring of its internal "east-west" traffic could have potentially detected anomalies in how the attackers were using its administrator tools, says John Burns, director of OT threat hunting for Dragos, an OT security firm. …

Source and more information:

https://www.darkreading.com/cybersecurity-operations/east-west-monitoring-visibility-critical-apt-detection

Cyber threats to rail, ports, airports could cripple US military mobilization, FDD report warns

A new report from the Cyberspace Solarium Commission reveals that U.S. adversaries are aware that targeting critical infrastructure through cyber and physical attacks could significantly hinder America's capacity to deploy, supply, and sustain large military forces. It also takes into account that a direct military engagement with a near-peer adversary would necessitate the rapid mobilization and deployment of a large U.S. military force. The efficient movement of troops and equipment across land, sea, and air is crucial for projecting power and supporting allies.

While U.S. Transportation Command (TRANSCOM) manages logistics, civilian-owned infrastructure, including rail networks, commercial ports, and airports, will primarily facilitate the transportation of servicemembers and materials during a swift mobilization. The FDD report also offers policy recommendations to strengthen cybersecurity for maritime, railroad, and aviation sectors. …

Source and more information:

https://industrialcyber.co/reports/cyber-threats-to-rail-ports-airports-could-cripple-us-military-mobilization-fdd-report-warns/

Emerging Risks Require IT/OT Collaboration to Secure Physical Systems

Education and awareness remain key to defending against cyberattacks against systems that disrupt operations or cause physical harm. Preventing cyber-physical attacks is not an impossible feat, but it requires greater collaboration between IT and operational technology (OT) professionals.

Attacks targeting vulnerabilities in physical systems, such as buildings, manufacturing equipment, sensors, and Internet of Things, can result in damaged equipment, theft or destruction or property, or injuries to people as a result of malfunctioning devices. Collaboration and awareness between IT and OT professionals are increasingly necessary because these cyber-physical attacks threaten both IT and OT sides. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/experts-discuss-current-and-emerging-ics-security-risks

Cyberattacks on water and power utilities threaten public safety

62% of utility operators were targeted by cyberattacks in the past year, and of those, 80% were attacked multiple times, according to Semperis. 54% suffered permanent corruption or destruction of data and systems.

Recent high-profile cyberattacks by nation-state groups on water and electricity utilities underscore the vulnerability of critical infrastructure. A public utility in Littleton, MA, was recently compromised by a group linked to Volt Typhoon, the Chinese state-sponsored threat group. American Water Works — the largest U.S. water and wastewater utility — also detected unauthorized activity in its computer network that disrupted customer service and billing. ...

Source and more information:

https://www.helpnetsecurity.com/2025/04/08/state-of-critical-infrastructure-resilience/

If Boards Don't Fix OT Security, Regulators Will

Around the world, governments are setting higher-bar regulations with clear corporate accountability for breaches on the belief organizations won't drive up security maturity for operational technology unless they're made to.

Lviv, Ukraine. Arkansas City, United States. Drum, Ireland. In each case, hackers broke in through exposed IT systems and found operational technology (OT) environments wide open: a pump controller or heating utility linked directly to the business network with no segmentation in sight. …

Source and more information:

https://www.darkreading.com/ics-ot-security/boards-fix-ot-security-regulators

Study Identifies 20 Most Vulnerable Connected Devices of 2025

Routers represent the riskiest devices in enterprise networks, containing the largest number of critical vulnerabilities, Forescout notes in a new report.

According to the company's 'Riskiest Connected Devices of 2025' report, device risk has increased 15% compared to the previous year, with routers accounting for more than half of the devices plagued by the most dangerous vulnerabilities.

The report, which analyzes millions of devices in Forescout's Device Cloud to identify the riskiest types across IT, IoT, OT, and Internet of Medical Things (IoMT), shows that computers have the largest number of bugs, but not the most dangerous ones. …

Source and more information:

https://www.securityweek.com/study-identifies-20-most-vulnerable-connected-devices-of-2025/

Integrating AI and ML technologies across OT, ICS environments to enhance anomaly detection and operational resilience

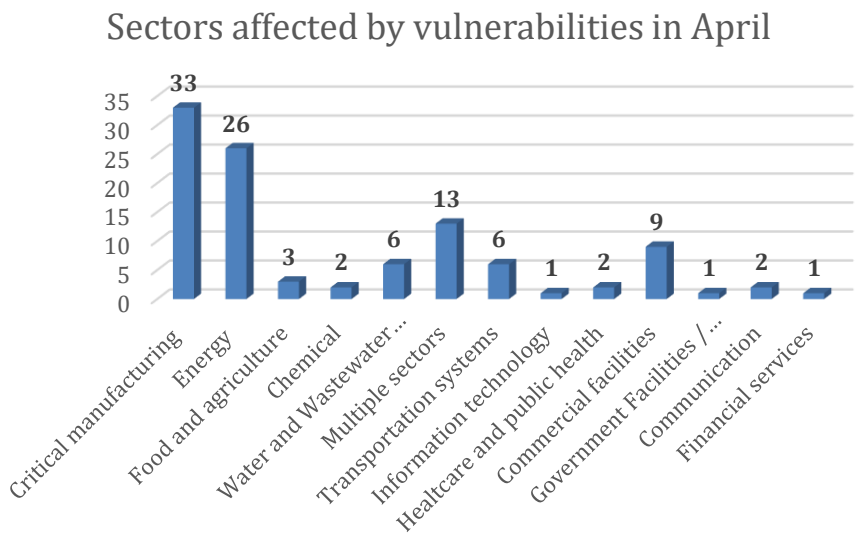
As the industrial cybersecurity landscape adopts AI and ML technologies, helping enhance anomaly detection across OT (operational technology) and ICS (industrial control systems) environments, they also improve capability visibility and response throughout the organizational systems lifecycle. Applying AI (artificial intelligence) in OT environments presents unique challenges, as the data preconditions are different. Relatively low complexity OT systems tend to yield noisy, unstructured, or incomplete data, necessitating specialized domain-knowledge filtering and extensive preprocessing. …

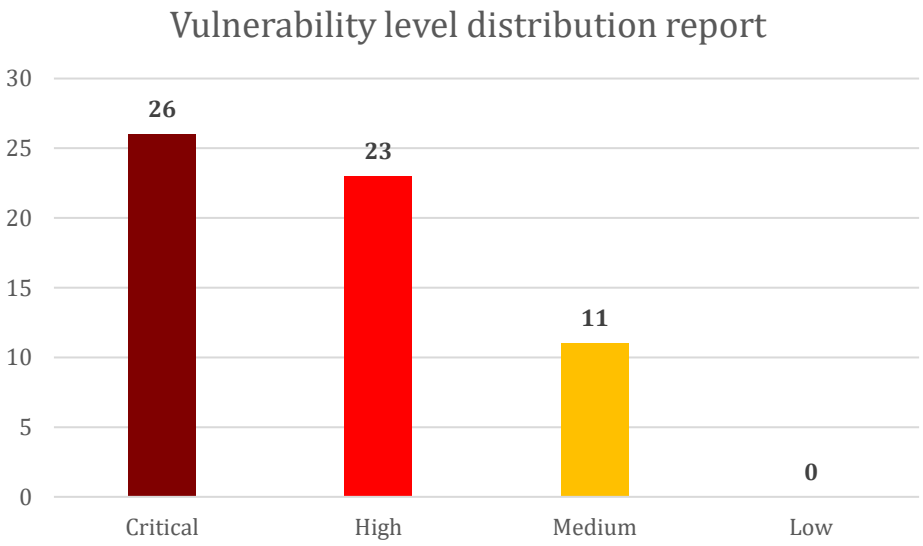
Source and more information:

https://industrialcyber.co/features/integrating-ai-and-ml-technologies-across-ot-ics-environments-to-enhance-anomaly-detection-and-operational-resilience/

ICS vulnerabilities

In April 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-25-119-01: **Rockwell Automation ThinManager**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Incorrect Default Permissions.

Rockwell Automation ThinManager | CISA

ICSA-25-119-02: **Delta Electronics ISPSoft**

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

Delta Electronics ISPSoft | CISA

ICSA-25-105-05: **Lantronix XPort (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Lantronix Xport (Update A) | CISA

ICSA-25-114-01: **Schneider Electric Modicon Controllers**

Critical level vulnerabilities: Trust Boundary Violation, Uncaught Exception, Exposure of Sensitive Information to an Unauthorized Actor, Authentication Bypass by Spoofing, Improper Access Control, Reliance on Untrusted Inputs in a Security Decision, Out-of-bounds Read.

Schneider Electric Modicon Controllers | CISA

ICSA-25-114-02: **ALBEDO Telecom Net.Time - PTP/NTP Clock**

High level vulnerability: Insufficient Session Expiration.

ALBEDO Telecom Net.Time - PTP/NTP Clock | CISA

ICSA-25-114-03: **Vestel AC Charger**

High level vulnerability: Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Vestel AC Charger | CISA

ICSA-25-114-04: **Nice Linear eMerge E3**

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

Nice Linear eMerge E3 | CISA

ICSA-25-114-05: **Johnson Controls ICU**

Critical level vulnerability: Stack-based Buffer Overflow.

Johnson Controls ICU | CISA

ICSA-25-114-06: **Planet Technology Network Products**

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

Planet Technology Network Products | CISA

ICSA-24-338-05: **Fuji Electric Monitouch V-SFT (Update A)**

High level vulnerability: Out-of-bounds Write.

Fuji Electric Monitouch V-SFT (Update A) | CISA

ICSA-25-112-01: **Siemens TeleControl Server Basic SQL**

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

Siemens TeleControl Server Basic SQL | CISA

ICSA-25-112-02: **Siemens TeleControl Server Basic**

Medium level vulnerability: Improper Handling of Length Parameter Inconsistency.

Siemens TeleControl Server Basic | CISA

ICSA-25-112-03: **Schneider Electric Wiser Home Controller WHC-5918A**

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

Schneider Electric Wiser Home Controller WHC-5918A | CISA

ICSA-25-112-04: **ABB MV Drives**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Out-of-bounds Write.

ABB MV Drives | CISA

ICSA-25-035-04: **Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC (Update A)**

High level vulnerability: Incorrect Calculation of Buffer Size.

Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC (Update A) | CISA

ICSA-25-107-01: **Schneider Electric Trio Q Licensed Data Radio**

Medium level vulnerabilities: Insecure Storage of Sensitive Information, Initialization of a Resource with an Insecure Default.

Schneider Electric Trio Q Licensed Data Radio | CISA

ICSA-25-107-02: **Schneider Electric Sage Series**

Critical level vulnerabilities: Out-of-bounds Write, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incorrect Default Permissions, Unchecked Return Value, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Out-of-bounds Read.

Schneider Electric Sage Series | CISA

ICSA-25-107-03: **Schneider Electric ConneXium Network Manager**

High level vulnerabilities: Files or Directories Accessible to External Parties, Improper Input Validation.

Schneider Electric ConneXium Network Manager | CISA

ICSA-25-107-04: **Yokogawa Recorder Products**

Critical level vulnerability: Missing Authentication for Critical Function.

Yokogawa Recorder Products | CISA

ICSA-24-326-04: **Schneider Electric Modicon M340, MC80, and Momentum Unity M1E (Update A)**

Critical level vulnerabilities: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Schneider Electric Modicon M340, MC80, and Momentum Unity M1E (Update A) | CISA

ICSA-25-058-01: **Schneider Electric Communication Modules for Modicon M580 and Quantum Controllers (Update A)**

Critical level vulnerability: Out-of-bounds Write.

Schneider Electric Communication Modules for Modicon M580 and Quantum Controllers (Update A)) | CISA

ICSA-25-105-01: **Siemens Mendix Runtime**

Medium level vulnerability: Observable Response Discrepancy.

Siemens Mendix Runtime | CISA

ICSA-25-105-02: **Siemens Industrial Edge Device Kit**

Critical level vulnerability: Weak Authentication.

Siemens Industrial Edge Device Kit | CISA

ICSA-25-105-03: **Siemens SIMOCODE, SIMATIC, SIPLUS, SIDOOR, SIWAREX**

Medium level vulnerability: Uncontrolled Resource Consumption.

Siemens SIMOCODE, SIMATIC, SIPLUS, SIDOOR, SIWAREX | CISA

ICSA-25-105-04: **Growatt Cloud Applications**

Critical level vulnerabilities: Cross-site Scripting, Authorization Bypass Through User-Controlled Key, Insufficient Type Distinction, External Control of System or Configuration Setting.

Growatt Cloud Applications | CISA

ICSA-25-105-05: **Lantronix Xport**

Critical level vulnerability: Missing Authentication for Critical Function.

Lantronix Xport | CISA

ICSA-25-105-06: **National Instruments LabVIEW**

High level vulnerability: Out-of-bounds Write.

National Instruments LabVIEW | CISA

ICSA-25-105-07: **Delta Electronics COMMGR**

Critical level vulnerability: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG).

Delta Electronics COMMGR | CISA

ICSA-25-105-08: **ABB M2M Gateway**

High level vulnerabilities: Integer Overflow or Wraparound, Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'), Unquoted Search Path or Element, Untrusted Search Path, Use After Free, Out-of-bounds Write, Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Missing Release of Memory after Effective Lifetime, Allocation of Resources Without Limits or Throttling, Improper Privilege Management, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Restriction of Operations within the Bounds of a Memory Buffer, Incorrect Calculation of Buffer Size,

Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Access of Resource Using Incompatible Type ('Type Confusion'), Improper Input Validation, Uncontrolled Resource Consumption, Observable Discrepancy, Generation of Error Message Containing Sensitive Information, Improper Authentication, Improper Validation of Integrity Check Value, Inadequate Encryption Strength, Improper Removal of Sensitive Information Before Storage or Transfer, Exposure of Sensitive Information to an Unauthorized Actor.

ABB M2M Gateway | CISA

ICSA-25-105-09: **Mitsubishi Electric Europe B.V. smartRTU**

Critical level vulnerabilities: Missing Authentication for Critical Function, OS Command Injection.

Mitsubishi Electric Europe B.V. smartRTU | CISA

ICSA-25-100-01: **Siemens License Server**

Medium level vulnerabilities: Improper Privilege Management, Improper Certificate Validation.

Siemens License Server | CISA

ICSA-25-100-02: **Siemens SIDIS Prime**

Critical level vulnerabilities: Race Condition Enabling Link Following, Improper Validation of Integrity Check Value, Unchecked Input for Loop Condition, Expected Behavior Violation, Incorrect Provision of Specified Functionality, Heap-based Buffer Overflow, Cleartext Transmission of Sensitive Information, Use After Free, NULL Pointer Dereference, Exposure of Sensitive Information to an Unauthorized Actor, Out-of-bounds Write, Improper Input Validation, Uncontrolled Resource Consumption.

Siemens SIDIS Prime | CISA

ICSA-25-100-03: **Siemens Solid Edge**

High level vulnerability: Out-of-bounds Write.

Siemens Solid Edge | CISA

ICSA-25-100-04: **Siemens Industrial Edge Devices**

Critical level vulnerability: Weak Authentication.

Siemens Industrial Edge Devices | CISA

ICSA-25-100-05: **Siemens Insights Hub Private Cloud**

Critical level vulnerabilities: Improper Input Validation, Improper Isolation or Compartmentalization.

Siemens Insights Hub Private Cloud | CISA

ICSA-25-100-06: **Siemens SENTRON 7KT PAC1260 Data Manager**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Missing Authentication for Critical Function, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Use of Hard-coded Credentials, Cross-Site Request Forgery (CSRF), Unverified Password Change.

Siemens SENTRON 7KT PAC1260 Data Manager | CISA

ICSA-25-100-07: **Rockwell Automation Arena**

High level vulnerabilities: Use of Uninitialized Variable, Out-of-bounds Write, Out-of-bounds Read, Stack-based Buffer Overflow.

Rockwell Automation Arena | CISA

ICSA-25-100-08: **Subnet Solutions PowerSYSTEM Center**

Medium level vulnerability: Out-of-Bounds Read, Deserialization of Untrusted Data.

Subnet Solutions PowerSYSTEM Center | CISA

ICSA-25-100-09: **ABB Arctic Wireless Gateways**

Critical level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Privilege Management, Exposure of Sensitive Information to an Unauthorized Actor, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

ABB Arctic Wireless Gateways | CISA

ICSMA-25-100-01: **INFINITT Healthcare INFINITT PACS**

High level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

INFINITT Healthcare INFINITT PACS | CISA

SSA-935500: **Siemens APOGEE, TALON and Desigo PXC/PXM Products (Update: 1.2.)** **High** level vulnerability: Uncontrolled Resource Consumption.

SSA-935500

SSA-913875: **Siemens SCALANCE W-700 IEEE 802.11n family 802.11 (Update: 1.4.)**

Medium level vulnerabilities: Missing Authentication for Critical Function, Improper Authentication, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Validation of Integrity Check Value, Improper Input Validation.

SSA-913875

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.5.)**

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

SSA-876787

SSA-770770: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.2.)**

Critical level vulnerabilities: Multiple.

SSA-770770

SSA-767615: **Siemens SIPROTEC 5 Devices (Update: 1.2.)**

High level vulnerability: Use of Default Credentials.

SSA-767615

SSA-698820: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.6.)**

High level vulnerabilities: Stack-based Buffer Overflow, Session Fixation, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authentication for Critical Function, Incorrect Parsing of Numbers with Different Radices, Improperly Implemented Security Check for Standard, Improper Access Control.

SSA-698820

SSA-686975: **Siemens Industrial Products using Intel CPUs (Update: 1.6.)**

High level vulnerability: Time-of-check Time-of-use (TOCTOU) Race Condition.

SSA-686975

SSA-503939: **Siemens SIMATIC S7-1500 TM MFP (Update: 1.1.)**

High level vulnerabilities: Multiple.

SSA-503939

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update: 2.5.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-369369: **Siemens SIMATIC IPC DiagMonitor (Update: 1.1.)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

SSA-369369

SSA-364175: **Siemens RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update: 1.5.)** **Critical** level vulnerabilities: Truncation of Security-relevant Information, Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Improper Input Validation, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Out-of-bounds Write, Improper Input Validation, Uncontrolled Resource Consumption.

SSA-364175

SSA-354569: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.3.)**

Critical level vulnerabilities: Missing Authentication for Critical Function, NULL Pointer Dereference, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Check for Unusual or Exceptional Conditions, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), External Control of File Name or Path, Improper Resolution of Path Equivalence.

SSA-354569

SSA-306654: **Siemens Industrial Products (Update: 1.9.)**

High level vulnerabilities: Multiple.

SSA-306654

SSA-265688: **Siemens SIMATIC S7-1500 TM MFP V1.1 (Update: 1.5.)**

Medium level vulnerabilities: Multiple.

SSA-265688

SSA-195895: **Siemens SIMATIC Products (Update: 1.2.)**

Medium level vulnerability: Observable Discrepancy.

SSA-195895

SSA-054046: **Siemens SIMATIC S7-1500 CPUs (Update: 1.4.)**

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

SSA-054046

ICSA-25-093-01: **Hitachi Energy RTU500 Series**

High level vulnerabilities: Null Pointer Dereference, Insufficient Resource Pool, Missing Synchronization.

Hitachi Energy RTU500 Series | CISA

ICSA-25-093-02: **Hitachi Energy TRMTracker**

Medium level vulnerabilities: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection'), Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Hitachi Energy TRMTracker | CISA

ICSA-25-093-03: **ABB ACS880 Drives Containing CODESYS RTS**

High level vulnerabilities: Improper Input Validation, Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer.

ABB ACS880 Drives Containing CODESYS RTS | CISA

ICSA-25-093-04: **ABB Low Voltage DC Drives and Power Controllers CODESYS RTS**

High level vulnerabilities: Improper Input Validation, Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer.

ABB Low Voltage DC Drives and Power Controllers CODESYS RTS | CISA

ICSA-25-093-05: **B&R APROL**

Critical level vulnerabilities: Inclusion of Functionality from Untrusted Control Sphere, Incomplete Filtering of Special Elements, Improper Control of Generation of Code ('Code Injection'), Improper Handling of Insufficient Permissions or Privileges , Allocation of Resources Without Limits or Throttling, Missing Authentication for Critical Function, Exposure of Sensitive System Information to an Unauthorized Control Sphere, Exposure of Data Element to Wrong Session, Server-Side Request Forgery (SSRF), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), External Control of File Name or Path, Incorrect Permission Assignment for Critical Resource.

B&R APROL | CISA

ICSA-25-091-01: **Rockwell Automation Lifecycle Services with Veeam Backup and Replication**

Critical level vulnerability: Deserialization of Untrusted Data.

Rockwell Automation Lifecycle Services with Veeam Backup and Replication | CISA

ICSA-24-331-04: **Hitachi Energy MicroSCADA Pro/X SYS600 (Update A)**

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

Hitachi Energy MicroSCADA Pro/X SYS600 (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 April:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-20439 Cisco Smart Licensing Utility Static Credential Vulnerability;
CVE-2025-24813 Apache Tomcat Path Equivalence Vulnerability;
CVE-2025-22457 Ivanti Connect Secure, Policy Secure and ZTA Gateways Stack-Based Buffer Overflow Vulnerability;
CVE-2025-31161 CrushFTP Authentication Bypass Vulnerability;
CVE-2025-30406 Gladinet CentreStack Use of Hard-coded Cryptographic Key Vulnerability;
CVE-2025-29824 Microsoft Windows Common Log File System (CLFS) Driver Use-After-Free Vulnerability;
CVE-2024-53197 Linux Kernel Out-of-Bounds Access Vulnerability;
CVE-2024-53150 Linux Kernel Out-of-Bounds Read Vulnerability;
CVE-2021-20035 SonicWall SMA100 Appliances OS Command Injection Vulnerability;
CVE-2025-31200 Apple Multiple Products Memory Corruption Vulnerability;
CVE-2025-31201 Apple Multiple Products Arbitrary Read and Write Vulnerability;
CVE-2025-24054 Microsoft Windows NTLM Hash Disclosure Spoofing Vulnerability;
CVE-2025-1976 Broadcom Brocade Fabric OS Code Injection Vulnerability;
CVE-2025-42599 Qualitia Active! Mail Stack-Based Buffer Overflow Vulnerability;
CVE-2025-3928 Commvault Web Server Unspecified Vulnerability;
CVE-2025-31324 SAP NetWeaver Unrestricted File Upload Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Vulnerability to the KEV Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

NSA, CISA, FBI, and International Partners Release Cybersecurity Advisory on "Fast Flux," a National Security Threat
CISA—in partnership with the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ)—released joint Cybersecurity Advisory Fast Flux: A National Security Threat (PDF, 841 KB). This advisory warns organizations, internet

service providers (ISPs), and cybersecurity service providers of the ongoing threat of fast flux enabled malicious activities and provides guidance on detection and mitigations to safeguard critical infrastructure and national security.
Links and more information:
NSA, CISA, FBI, and International Partners Release Cybersecurity Advisory on "Fast Flux," a National Security Threat | CISA

Fortinet Releases Advisory on New Post-Exploitation Technique for Known Vulnerabilities
Fortinet is aware of a threat actor creating a malicious file from previously exploited Fortinet vulnerabilities (CVE-2024-21762, CVE-2023-27997, and CVE-2022-42475) within FortiGate products. This malicious file could enable read-only access to files on the device's file system, which may include configurations. Fortinet has communicated directly with the account holders of customers identified as impacted by this issue based on the available telemetry with mitigation guidance.
Links and more information:
Fortinet Releases Advisory on New Post-Exploitation Technique for Known Vulnerabilities | CISA

CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise
CISA is aware of public reporting regarding potential unauthorized access to a legacy Oracle cloud environment. While the scope and impact remains unconfirmed, the nature of the reported activity presents potential risk to organizations and individuals, particularly where credential material may be exposed, reused across separate, unaffiliated systems, or embedded (i.e., hardcoded into scripts, applications, infrastructure templates, or automation tools). When credential material is embedded, it is difficult to discover and can enable long-term unauthorized access if exposed.
Links and more information:
CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise | CISA