2025 March, Industrial Control Systems security feed

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

List of Contents

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

OT Cybersecurity Year in Review & Key Takeaways for 2025

Secomea published an article, which presenting 8 major trends in OT cybersecurity and 8 mitigation strategies that manufacturers and machine builders can adopt to counter OT cybersecurity challenges.

8 major trends:

1. The rise of ransomware attacks and ICS intrusions
2. Critical infrastructure risks persist in the industry
3. The impact of global IT outages on OT environments
4. The exploitation of IT-centric remote access technologies
5. Regulators across regions are focusing on OT cybersecurity
6. Zero-Trust gaining momentum across Europe and the US
7. Heightened emphasis on supply chain security
8. Worldwide shortage of OT cybersecurity professionals

8 mitigation strategies:

1. Implement Zero Trust Architectures (ZTA)
2. Establish a patch management policy specific to OT environments
3. Invest in advanced monitoring solutions and SIEM for OT
4. Strengthen remote access security
5. Cover both IT and OT systems in your regular security assessments
6. Continuously review your incident response plan and conduct regular cybersecurity drills to test it
7. Train and educate the workforce on OT-specific risks
8. Prioritize supply chain security and regulatory compliance

Strongly recommend to read the whole article in this hot topic!

Source and more detailed information available on the following link:

https://secomea.com/remote-access/ot-cybersecurity-year-in-review-and-key-takeaways-for-2025/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in April 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 April 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

The 6th Annual CS4CA APAC Summit

The joint events CS4CA APAC & APAC Cyber Summit bring together over 150 senior cyber security leaders and decision-makers from critical industries such as oil & gas, mining, utilities, manufacturing and transportation, as well as finance, healthcare, retail and more, to connect, learn, be inspired and collaborate on building cyber resilience.

We will be exploring the most important developments in Asia-Pacific security strategies, tools and standards, over two days packed with both networking and educational sessions — including an exclusive deep dive into Singapore's OT Cybersecurity Masterplan, delivered by the Cyber Security Agency of Singapore.

Marina Bay Sands, Singapore; 16th - 17th April 2025

More details can be found on the following website:

https://apac.cs4ca.com/

OT.SEC.CON. Operate & Secure

OT.SEC.CON. is THE Houston-area OT security conference where operational technology meets cybersecurity in a groundbreaking event designed to bridge the gap between owner/operators and cybersecurity experts. The mission is to facilitate conversations between these roles to foster a deeper understanding of the challenges in industrial environments from both perspectives. By bringing these two worlds together, OT.SEC.CON aims to build a collaborative community that can collectively defend critical infrastructure.

Houston Texas, USA; 17th April 2025

More details can be found on the following website:

https://www.otseccon.com/

ICS incidents

Cyberattack disrupts Lee newspapers' operations across the US

Lee Enterprises, one of the largest newspaper groups in the United States, experienced a significant cyberattack on February 3, 2025, leading to an extensive outage that disrupted its operations. The company disclosed the incident in a filing with the U.S. Securities and Exchange Commission (SEC) on Friday, confirming that the cyber event severely impacted its business applications and resulted in an operational shutdown.

Following the attack, Lee Enterprises has been working to assess the scope of the incident, particularly whether any sensitive information was compromised. A spokesperson for the company emphasized that the investigation is ongoing and complex, potentially taking several weeks or longer to complete. The company has also notified law enforcement authorities about the breach.

The cyberattack forced the shutdown of numerous networks, causing disruptions in the printing and delivery of multiple newspapers. VPN access was also affected, leaving reporters and editors unable to retrieve critical files. Several Lee Enterprises publications displayed website banners informing readers of temporary service interruptions affecting subscription accounts and digital editions.

Lee Enterprises operates 77 daily newspapers and over 350 weekly and specialty publications across 26 states. Its print circulation surpasses 1.2 million, while digital editions attract over 44 million unique visitors. Notable newspapers under its ownership include the Buffalo News (New York), the Richmond Times-Dispatch (Virginia), the Arizona Daily Star, the Omaha World-Herald (Nebraska), and the St. Louis Post-Dispatch (Missouri), among others.

This is not the first cyberattack targeting Lee Enterprises. In 2019, Iranian hackers breached the company's network as part of a disinformation campaign ahead of the 2020 U.S. presidential election. The latest attack underscores ongoing cybersecurity threats facing media organizations and the potential impact on their operations.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/cyberattack-disrupts-lee-newspapers-operations-across-the-us/

Book recommendation

Intelligent Cyber-Physical Systems Security for Industry 4.0: Applications, Challenges and Management

Intelligent Cyber-Physical Systems Security for Industry 4.0: Applications, Challenges and Management presents new cyber-physical security findings for Industry 4.0 using emerging technologies like Artificial Intelligence (with Machine / Deep Learning), Data Mining, Applied Mathematics. All these are the essential components for processing data, recognizing patterns, modelling new techniques, and improving the advantages of the Data Science more. Features

- Presents an integrated approach with Cyber-Physical Systems, CPS security, and Industry 4.0 in one place
- Exposes the necessity of security initiatives, standards, security policies, and procedures in the context of industry 4.0
- Suggests solutions for enhancing the protection of 5G and the Internet of Things (IoT) security
- Promotes how optimization or intelligent techniques envisage the role of Artificial Intelligence-Machine / Deep Learning (AI-ML/DL) in cyberphysical systems security for industry 4.0

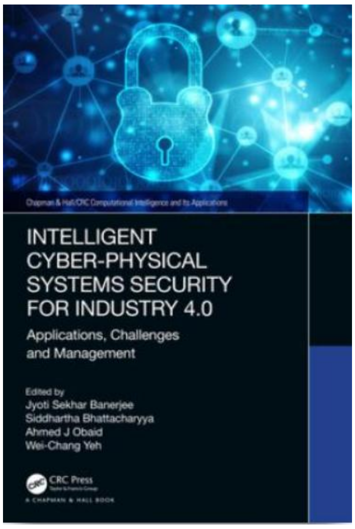
This book is primarily aimed at graduates, researchers and professionals working in the field of security. Executives concerned with the security management, knowledge dissemination, information, and policy development for data and network security in different educational, government, and non-government organizations will also find this book useful.

Author/Editor: Banerjee Jyoti Sekhar

Year of issue: 2022

The book is available at the following link:

https://www.enbook.hu/catalog/product/view/id/2143093?utm_source=google&utm_medium=cpc&utm_campaign=Enbook%20HU%20-%20PMAX_All%20products&utm_id=21584152069&gad_source=1&gclid=CjwKCAiAw5W-BhAhEiwApv4goIQ2iWQLVnO5aC8ZFlgIxZBc2q3B7niHYgeaMhOukZb7-3Pr23wW3RoCEm4QAvD_BwE


Chapman & Hall/CRC Computational Intelligence and Its Applications
INTELLIGENT CYBER-PHYSICAL SYSTEMS SECURITY FOR INDUSTRY 4.0
Applications, Challenges and Management
Edited by
Jyoti Sekhar Banerjee
Siddhartha Bhattacharyya
Ahmed J Obaid
Wei-Chang Yeh
CRC Press
A CHAPMAN & HALL BOOK

ICS security news selection

OT/ICS cyber threats escalate as geopolitical conflicts intensify

Ransomware attacks against industrial organizations surged by 87% over the past year, while new malware families designed specifically for OT environments emerged. These findings highlight a troubling trend: OT systems are increasingly becoming mainstream targets, and even sophisticated threat actors use relatively unsophisticated tactics to infiltrate and disrupt industrial operations.

State-sponsored groups embed themselves in critical infrastructure, while hacktivists and cybercriminals exploit known vulnerabilities, weak remote access configurations, and exposed OT assets. A persistent lack of visibility into OT environments continues to obscure the full scale of these attacks. These insights come from Dragos' 2025 OT/ICS Cybersecurity Report, its eighth annual Year in Review, which analyzes industrial organizations' cyber threats. …

Source and more information:

https://www.helpnetsecurity.com/2025/02/28/dragos-2025-ot-ics-cybersecurity-report/

Nine Threat Groups Active in OT Operations in 2024: Dragos

Industrial cybersecurity company Dragos on Tuesday published its 2025 OT/ICS Cybersecurity Report, which provides insights on the threat activity and trends observed last year.

Dragos tracks a total of 23 threat groups that have targeted OT organizations over the past years, and nine of them were active in 2024.

Two of them are newly added groups. One of them has been named Bauxite, which has been linked to Iran. Operating under the hacktivist persona CyberAv3ngers, Bauxite has targeted organizations in the US, Europe, Australia and the Middle East, including sectors such as energy, water, food and beverage, and chemical manufacturing. …

Source and more information:

https://www.securityweek.com/nine-threat-groups-active-in-ot-operations-in-2024-dragos/

Armis Acquires OTORIO to Expand OT Exposure Management Platform

Operational technology (OT) exposure management provider Armis acquired OTORIO, marking its third acquisition in the past year. While the terms of the deal were not disclosed, several reports estimate Armis paid $120 million based on market estimates.

Founded in 2018, OTORIO specializes in OT cybersecurity, focusing on industrial control systems and cyber-physical systems. Armis said it intends to integrate OTORIO’s Titan, an on-premise platform providing exposure management, threat detection, and secure access management for IoT and OT networks, with Armis’ Centrix, its cloud-based OT and Cyber Physical Systems security platform. …

Source and more information:

https://www.darkreading.com/ics-ot-security/armis-acquires-otorio-expand-ot-exposure-management-platform

MITRE EMB3D for OT & ICS Threat Modeling Takes Flight

Frameworks to aid device and industrial control system (ICS) manufacturers in modeling the threats that their products face continue to gain traction as research matures.

Non-profit government research organization MITRE, for example, announced its EMB3D framework for threat modeling in late 2023, outlining specific categories of threats. Late last year, MITRE added recommendations for companies to mitigate the threats. And already, device manufacturers are starting to use EMB3D to enhance their threat modeling processes, researchers are using it to discuss findings in the same language, and cybersecurity vendors have started incorporating it into the products, says Marie Stanley Collins, senior principal with MITRE's Critical Infrastructure Initiative. …

Source and more information:

https://www.darkreading.com/threat-intelligence/mitre-emb3d-ot-ics-threat-modeling

Switzerland mandates 24-hour cyberattack reporting for critical infrastructure operators from April

The Switzerland National Cyber Security Centre (NCSC) has introduced a mandatory reporting requirement for cyberattacks targeting critical infrastructure, effective from

April 1. Critical infrastructure operators must report any cyberattacks to the NCSC within 24 hours of detection. The reporting requirement is set out in the Information Security Act (ISA) and the Cybersecurity Ordinance (CSO). Also, these reports will allow the NCSC to support victims of cyberattacks and notify other critical infrastructure operators.

Additionally, the NCSC's Federal Council has decided to implement the relevant legislation for fines on Oct. 1 to give those concerned sufficient time to prepare for the new reporting obligation. This means that the reporting obligation will apply for six months before failure to report becomes sanctionable. …

Source and more information:

https://industrialcyber.co/regulation-standards-and-compliance/switzerland-mandates-24-hour-cyberattack-reporting-for-critical-infrastructure-operators-from-april/

Belgium's CCB reports significant registration surge under NIS2, as 2,410 organizations from critical sectors enrolled

The Center for Cybersecurity Belgium (CCB) announced on Monday that since the implementation of the NIS2 legislation last October, 2,410 organizations from critical sectors have registered, contributing to a total of over 4,500 organizations across various sectors. The initiative signifies the launch of the most extensive cybersecurity initiative in the country's history.

According to an estimate based on figures from the FPS Economy, approximately 2,500 organizations fall within the scope of NIS2. Consequently, it can be concluded that the vast majority have timely aligned themselves by registering. …

Source and more information:

https://industrialcyber.co/regulation-standards-and-compliance/belgiums-ccb-reports-significant-registration-surge-under-nis2-as-2410-organizations-from-critical-sectors-enrolled/

OT systems are strategic targets in global power struggles

Compared to 2023, 2024 saw a smaller increase in cyberattacks that caused physical consequences on OT organizations, according to Waterfall Security. Nevertheless, there were sharp jumps in the number of sites affected by the hacks, as well as in the number of attacks by nation states.

2024 saw a 146% increase in sites suffering physical consequences of operations because of cyberattacks, rising from 412 sites in 2023 to 1,015 in 2024.

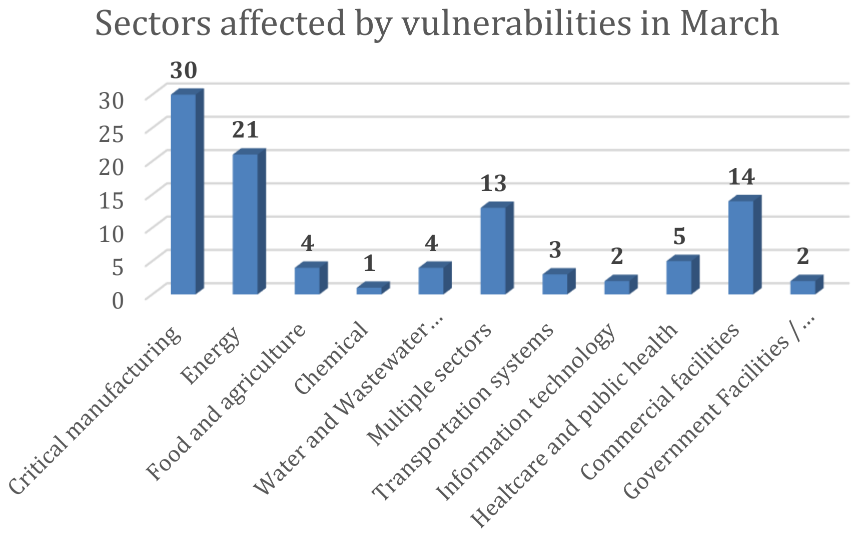
The slowing rate of increase in OT security incidents may be due to new SEC disclosure regulations, which require publicly traded companies to report “material” cybersecurity incidents. …

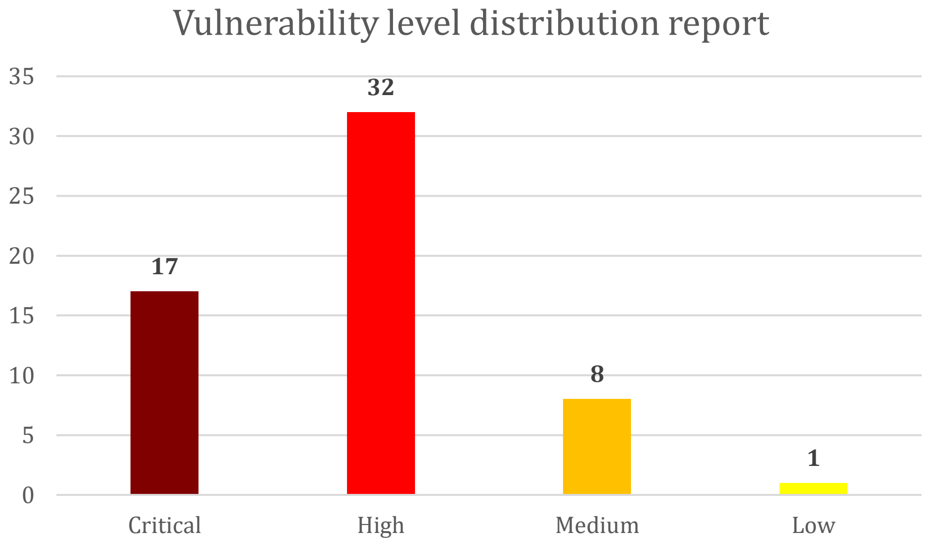
Source and more information:

https://www.helpnetsecurity.com/2025/03/25/cyberattacks-physical-consequences-ot-organizations/

ICS vulnerabilities

In March 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-25-037-011. **Schneider Electric EcoStruxure Power Monitoring Expert (PME) (Update A)**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Monitoring Expert (PME) (Update A) | CISA

ICSA-25-084-01: **ABB RMC-100**

High level vulnerability: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution').

ABB RMC-100 | CISA

ICSA-25-084-02: **Rockwell Automation Verve Asset Manager**

High level vulnerability: Improper Validation of Specified Type of Input.

Rockwell Automation Verve Asset Manager | CISA

ICSA-25-084-03: **Rockwell Automation 440G TLS-Z**

High level vulnerability: Improper Neutralization of Special Elements in Output Used by a Downstream Component.

Rockwell Automation 440G TLS-Z | CISA

ICSA-25-084-04: **Inaba Denki Sangyo CHOCO TEI WATCHER Mini**

Critical level vulnerabilities: Use of Client-Side Authentication, Storing Passwords in a Recoverable Format, Weak Password Requirements, Direct Request ('Forced Browsing').

Inaba Denki Sangyo CHOCO TEI WATCHER Mini | CISA

ICSA-25-079-01: **Schneider Electric EcoStruxure™**

High level vulnerability: Improper Privilege Management.

Schneider Electric EcoStruxure™ | CISA

ICSA-25-079-02: **Schneider Electric Enerlin'X IFE and eIFE**

High level vulnerability: Improper Input Validation.

Schneider Electric Enerlin'X IFE and eIFE | CISA

ICSA-25-079-03: **Siemens Simcenter Femap**

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

Siemens Simcenter Femap | CISA

ICSA-25-079-04: **SMA Sunny Portal**

Medium level vulnerability: Unrestricted Upload of File with Dangerous Type.

SMA Sunny Portal | CISA

ICSMA-25-079-01: **Santesoft Sante DICOM Viewer Pro**

High level vulnerability: Out-of-Bounds Write.

Santesoft Sante DICOM Viewer Pro | CISA

ICSA-25-077-01: **Schneider Electric EcoStruxure Power Automation System User Interface (EPAS-UI)**

High level vulnerability: Improper Authentication.

Schneider Electric EcoStruxure Power Automation System User Interface (EPAS-UI) | CISA

ICSA-25-077-02: **Rockwell Automation Lifecycle Services with VMware**

Critical level vulnerabilities: Time-of-check Time-of-use (TOCTOU) Race Condition, Write-what-where Condition, Out-of-bounds Read.

Rockwell Automation Lifecycle Services with VMware | CISA

ICSA-25-077-03: **Schneider Electric EcoStruxure Power Automation System**

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

Schneider Electric EcoStruxure Power Automation System | CISA

ICSA-25-077-04: **Schneider Electric EcoStruxure Panel Server**

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

Schneider Electric EcoStruxure Panel Server | CISA

ICSA-25-077-05: **Schneider Electric ASCO 5310/5350 Remote Annunciator**

High level vulnerabilities: Download of Code Without Integrity Check, Allocation of Resources Without Limits or Throttling, Cleartext Transmission of Sensitive Information, Unrestricted Upload of File with Dangerous Type.

Schneider Electric ASCO 5310/5350 Remote Annunciator | CISA

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

Critical level vulnerability: Improper Input Validation.

Schneider Electric Modicon (Update A) | CISA

ICSA-24-291-03: **Mitsubishi Electric CNC Series (Update B)**

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

Mitsubishi Electric CNC Series (Update B) | CISA

ICSA-25-072-01: **Siemens Teamcenter Visualization and Tecnomatrix Plant Simulation**

High level vulnerabilities: Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Read, Use After Free.

Siemens Teamcenter Visualization and Tecnomatrix Plant Simulation | CISA

ICSA-25-072-02: **Siemens SINEMA Remote Connect Server**

High level vulnerabilities: Improper Output Neutralization for Logs, Missing Release of Resource after Effective Lifetime.

Siemens SINEMA Remote Connect Server | CISA

ICSA-25-072-03: **Siemens SIMATIC S7-1500 TM MFP**

High level vulnerabilities: Double Free, Use After Free, NULL Pointer Dereference, Buffer Access with Incorrect Length Value, Use of Uninitialized Variable.

Siemens SIMATIC S7-1500 TM MFP | CISA

ICSA-25-072-04: **Siemens SiPass integrated AC5102/ACC-G2 and ACC-AP**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Input Validation.

Siemens SiPass integrated AC5102/ACC-G2 and ACC-AP | CISA

ICSA-25-072-05: **Siemens SINAMICS S200**

Critical level vulnerability: Improper Authentication.

Siemens SINAMICS S200 | CISA

ICSA-25-072-06: **Siemens SCALANCE LPE9403**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Check for Dropped Privileges.

Siemens SCALANCE LPE9403 | CISA

ICSA-25-072-07: **Siemens SCALANCE M-800 and SC-600 Families**

Medium level vulnerability: Partial String Comparison.

Siemens SCALANCE M-800 and SC-600 Families | CISA

ICSA-25-072-08: **Siemens Tecnomatix Plant Simulation**

High level vulnerability: Files or Directories Accessible to External Parties.

Siemens Tecnomatix Plant Simulation | CISA

ICSA-25-072-09: **Siemens OPC UA**

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

Siemens OPC UA | CISA

ICSA-25-072-10: **Siemens SINEMA Remote Connect Client**

Critical level vulnerabilities: Integer Overflow or Wraparound, Unprotected Alternate Channel, Improper Restriction of Communication Channel to Intended Endpoints, Stack-based Buffer Overflow, Unrestricted Upload of File with Dangerous Type, Missing Release of Resource after Effective Lifetime.

Siemens SINEMA Remote Connect Client | CISA

ICSA-25-072-11: **Siemens SIMATIC IPC Family, ITP1000, and Field PGs**

High level vulnerability: Protection Mechanism Failure.

Siemens SIMATIC IPC Family, ITP1000, and Field PGs | CISA

ICSA-25-072-12: **Sungrow iSolarCloud Android App and WiNet Firmware**

Critical level vulnerabilities: Improper Certificate Validation, Use of a Broken or Risky Cryptographic Algorithm, Authorization Bypass Through User-Controlled Key, User of Hard-Coded Credentials, Stack-Based Buffer Overflow, Heap-Based Buffer Overflow.

Sungrow iSolarCloud Android App WiNet Firmware | CISA

ICSMA-25-072-01: **Philips Intellispace Cardiovascular (ISCV)**

High level vulnerabilities: Improper Authentication, Use of Weak Credentials.

Philips Intellispace Cardiovascular (ISCV) | CISA

SSA-928984: **Siemens User Management Component (UMC)** **(Update: 1.1.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-928984

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.4.)**

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

SSA-876787

SSA-832273: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.7.)**

Critical level vulnerabilities: Multiple.

SSA-832273

SSA-770770: **Siemens RUGGEDCOM APE1808 Devices (Update: 1.1.)**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read, Incorrect Privilege Assignment, Insertion of Sensitive Information Into Sent Data, Allocation of Resources Without Limits or Throttling, Integer Overflow or Wraparound, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Out-of-bounds Write, Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting').

SSA-770770

SSA-767615: **Siemens SIPROTEC 5 Devices (Update: 1.1.)**

High level vulnerability: Use of Default Credentials.

SSA-767615

SSA-723487: **Siemens SCALANCE, RUGGEDCOM and Related Products (Update: 1.5.)** **Critical** level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-620288: **Capital Embedded AR Classic (Update: 1.3.)**

High level vulnerabilities: Access of Resource Using Incompatible Type ('Type Confusion'), Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Restriction of Operations within the Bounds of a Memory Buffer, Integer Underflow (Wrap or Wraparound), Improper Handling of Inconsistent Structural Elements.

SSA-620288

SSA-593272: **Siemens Industrial Devices (Update: 2.4.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-593272

SSA-434032: **DHCP Client of Nucleus RTOS (Update: 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-434032

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update: 2.4.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-265688: **Siemens SIMATIC S7-1500 TM MFP V1.1 (Update: 1.4.)**

High level vulnerabilities: Multiple.

SSA-265688

SSA-248289: **IPv6 Stack of Nucleus RTOS (Update: 1.3.)**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

SSA-248289

SSA-195895: **Webserver of Siemens SIMATIC Products (Update: 1.1.)**

Medium level vulnerability: Observable Discrepancy.

SSA-195895

SSA-194557: **Siemens SIPROTEC 5 (Update: 1.2.)**

High level vulnerability: Files or Directories Accessible to External Parties.

SSA-194557

SSA-054046: **Web Server of Siemens SIMATIC S7-1500 CPUs (Update: 1.3.)**

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

SSA-054046

SSA-039007: **Siemens User Management Component (UMC) (Update: 1.4.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-039007

ICSA-25-070-01: **Schneider Electric Uni-Telway Driver**

Medium level vulnerability: Improper Input Validation.

Schneider Electric Uni-Telway Driver | CISA

ICSA-25-070-02: **Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool**

Critical level vulnerabilities: Use of Hard-coded, Security-relevant Constants, Authentication Bypass Using an Alternate Path or Channel.

Optigo Networks Visual BACnet Capture Tool/Optigo Visual Networks Capture Tool | CISA

ICSA-25-065-01: **Hitachi Energy PCU400**

High level vulnerabilities: Access of Resource Using Incompatible Type ('Type Confusion'), NULL Pointer Dereference, Use After Free, Double Free, Observable Discrepancy, Out-of-bounds Read.

Hitachi Energy PCU400 | CISA

ICSA-25-065-02: **Hitachi Energy Relion 670/650/SAM600-IO**

High level vulnerability: Improper Handling of Insufficient Privileges.

Hitachi Energy Relion 670/650/SAM600-IO | CISA

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

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Monitoring Expert (PME) | CISA

ICSA-25-063-01: **Carrier Block Load**

High level vulnerability: Uncontrolled Search Path Element.

Carrier Block Load | CISA

ICSA-25-063-02: **Keysight Ixia Vision Product Family**

High level vulnerabilities: Path Traversal, Improper Restriction of XML External Entity Reference.

Keysight Ixia Vision Product Family | CISA

ICSA-25-063-03: **Hitachi Energy MACH PS700**

Medium level vulnerability: Uncontrolled Search Path Element.

Hitachi Energy MACH PS700 | CISA

ICSA-25-063-04: **Hitachi Energy XMC20**

Medium level vulnerability: Relative Path Traversal.

Hitachi Energy XMC20 | CISA

ICSA-25-063-05: **Hitachi Energy UNEM/ECST**

Medium level vulnerability: Improper Validation of Certificate with Host Mismatch.

Hitachi Energy UNEM/ECST | CISA

ICSA-25-063-06: **Delta Electronics CNCSoft-G2**

High level vulnerability: Heap-based Buffer Overflow.

Delta Electronics CNCSoft-G2 | CISA

ICSA-25-063-07: **GMOD Apollo**

Critical level vulnerabilities: Incorrect Privilege Assignment, Relative Path Traversal, Missing Authentication for Critical Function, Generation of Error Message Containing Sensitive Information.

GMOD Apollo | CISA

ICSA-25-063-08: **Edimax IC-7100 IP Camera**

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

Edimax IC-7100 IP Camera | 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 March:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-20118 Cisco Small Business RV Series Routers Command Injection Vulnerability;
CVE-2022-43939 Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability;
CVE-2022-43769 Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability;
CVE-2018-8639 Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability;
CVE-2024-4885 Progress WhatsUp Gold Path Traversal Vulnerability;
CVE-2024-50302 Linux Kernel Use of Uninitialized Resource Vulnerability;
CVE-2025-22225 VMware ESXi Arbitrary Write Vulnerability;
CVE-2025-22224 VMware ESXi and Workstation TOCTOU Race Condition Vulnerability;
CVE-2025-22226 VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability;
CVE-2025-25181 Advantive VeraCore SQL Injection Vulnerability;
CVE-2024-57968 Advantive VeraCore Unrestricted File Upload Vulnerability;
CVE-2024-13159 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability;
CVE-2024-13160 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability;
CVE-2024-13161 Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability;
CVE-2025-24983 Microsoft Windows Win32k Use-After-Free Vulnerability;
CVE-2025-24984 Microsoft Windows NTFS Information Disclosure Vulnerability;
CVE-2025-24985 Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability;
CVE-2025-24991 Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability;
CVE-2025-24993 Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability;
CVE-2025-26633 Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability;
CVE-2025-24201 Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability;
CVE-2025-21590 Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability;
CVE-2025-24472 Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability;
CVE-2025-30066 tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability;
CVE-2025-1316 Edimax IC-7100 IP Camera OS Command Injection Vulnerability;
CVE-2024-48248 NAKIVO Backup and Replication Absolute Path Traversal Vulnerability;
CVE-2017-12637 SAP NetWeaver Directory Traversal Vulnerability;

CVE-2025-30154 reviewdog action-setup GitHub Action Embedded Malicious Code Vulnerability;
CVE-2019-9874 Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability;
CVE-2019-9875 Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability;
CVE-2025-2783 Google Chromium Mojo Sandbox Escape Vulnerability;
Links and more information:
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

FBI Warns of Data Extortion Scam Targeting Corporate Executives
The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) has released an alert warning of a scam involving criminal actors masquerading as the "BianLian Group." The cyber criminals target corporate executives by sending extortion letters threatening to release victims' sensitive information unless payment is received.
Links and more information:
FBI Warns of Data Extortion Scam Targeting Corporate Executives | CISA

CISA and Partners Release Cybersecurity Advisory on Medusa Ransomware
CISA—in partnership with the Federal Bureau of Investigation (FBI) and Multi-State Information Sharing and Analysis Center (MS-ISAC)—released joint Cybersecurity Advisory, #StopRansomware: Medusa Ransomware. This advisory provides tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and detection methods associated with known Medusa ransomware activity.
Links and more information:
CISA and Partners Release Cybersecurity Advisory on Medusa Ransomware | CISA

Supply Chain Compromise of Third-Party GitHub Action, CVE-2025-30066
A popular third-party GitHub Action, tj-actions/changed-files (tracked as CVE-2025-30066), was compromised. This GitHub Action is designed to detect which files have changed in a pull request or commit. The supply chain compromise allows for information disclosure of secrets including, but not limited to, valid access keys, GitHub Personal Access Tokens (PATs), npm tokens, and private RSA keys. This has been patched in v46.0.1.

Links and more information:
[Supply Chain Compromise of Third-Party GitHub Action, CVE-2025-30066 | CISA]

CISA Releases Malware Analysis Report on RESURGE Malware Associated with Ivanti Connect Secure

CISA has published a Malware Analysis Report (MAR) with analysis and associated detection signatures on a new malware variant CISA has identified as RESURGE. RESURGE contains capabilities of the SPAWNCHIMERA malware variant, including surviving reboots; however, RESURGE contains distinctive commands that alter its behavior.

Links and more information:
[CISA Releases Malware Analysis Report on RESURGE Malware Associated with Ivanti Connect Secure | CISA]