2025 June, 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

AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems

CISA, the National Security Agency, the Federal Bureau of Investigation, and international partners released *AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems*.

This guidance highlights the critical role of data security in ensuring the accuracy, integrity, and trustworthiness of AI outcomes. It outlines key risks that may arise from data security and integrity issues across all phases of the AI lifecycle, from development and testing to deployment and operation.

Source (the link) and more detailed information available on the following link:

AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems | CISA

ICS conferences

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

OTSEC MENA Summit & Awards

With the steady adoption of IoT and personal connected devices, it's reported an increase of over 4-fold in IoT malware attacks year-over-year in the Middle East region. The growth in cyber threats demonstrates cyber criminals' persistence and ability to adapt to evolving conditions in launching IoT malware attacks. Cybercriminals are targeting legacy vulnerabilities, with 34 of the 39 most popular IoT exploits specifically directed at vulnerabilities that have existed for over three years. The biggest receiver of these attacks has been manufacturing, followed by oil & gas, Power grids and maritime. Secured Managed Services and Ai will play a key role in the future of cyber security; however, it remains that it's not the task of the security team alone. It's an effort by everyone working within those organisations.

Join CISOs, Heads of OT and ICS Security from MENA region on 2nd July 2025, to discuss key challenges and opportunities in OT, IOT, IIOT & IOMT Cyber Security for Critical Infrastructure and key sectors at OTSEC MENA SUMMIT & AWARDS 2025.

Al Khobar, Saudi Arabia, 2nd July 2025

More details can be found on the following website:

https://otsecsummit.com/#agenda

EnergySec's 20th Security & Compliance Summit

Annual Summit has garnered praise from participants and sponsors alike within the energy sector for its insightful discussions, valuable networking opportunities, and impactful presentations. The 20th Anniversary promises to be our most dynamic and memorable event yet, filled with innovative sessions and exciting new elements including new Networking Events!

Anaheim, California, US: 15th -17th June | Courses: 28th -30th July 2025

More details can be found on the following website:

https://www.eventzilla.net/e/energysecs-20th-security--compliance-summit-2138627720?resp=on&dateid=2138256854

ICS incidents

Big Steelmaker Halts Operations After Cyber Incident

Nucor Corporation, a major steel manufacturer headquartered in North Carolina, has temporarily halted its production operations following a significant cybersecurity incident. According to the company's recent 8-K filing with the U.S. Securities and Exchange Commission, an unauthorized third party gained access to Nucor's IT systems. In response, Nucor immediately activated its incident response plan and took offline any systems that might have been compromised.

While specific details regarding the nature of the attack and the affected sites have not been disclosed, the company has confirmed that it is working with third-party cybersecurity experts and federal law enforcement agencies to investigate the breach. The production pause indicates that the attack may have extended beyond traditional IT infrastructure and potentially impacted Operational Technology (OT) systems - which are critical for controlling physical industrial processes.

This disruption is especially concerning given Nucor's role in U.S. critical infrastructure. With approximately 25,000 employees and first-quarter 2025 net sales of $7.83 billion, the company represents a high-value target for advanced threat actors. Although no specific group has been named, state-linked actors such as Volt Typhoon and Salt Typhoon are considered likely candidates, particularly due to their focus on compromising critical infrastructure sectors.

The Cybersecurity and Infrastructure Security Agency (CISA), alongside the FBI, Department of Energy, and Environmental Protection Agency, has issued ongoing warnings about the vulnerability of operational technology and industrial control systems within critical infrastructure. The Nucor incident underscores these concerns, as even partial compromise of OT environments can lead to serious operational disruptions and economic consequences.

Nucor has stated it is currently in the process of restoring the affected systems, but the full impact on its business continuity remains to be seen.

The source is available on the following link:

Big Steelmaker Halts Operations After Cyber Incident

Book recommendation

A Guide to Cybersecurity for Water and Wastewater Utilities

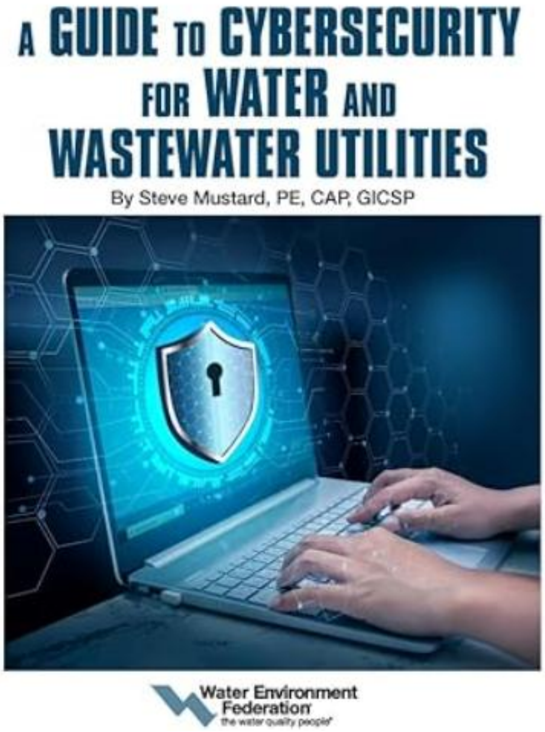
This book is intended to help water and wastewater utility managers and operators navigate the complex world of cybersecurity. It provides accessible guidance on how utilities of all sizes can manage their risks, focus their resources, and implement controls to keep their facilities and their communities safe. This includes creating a culture of good cybersecurity internally and managing relations with third-party contractors.

Author/Editor: Steve Mustard (Author)

Year of issue: 2024

The book is available at the following link:

https://www.amazon.com/Guide-Cybersecurity-Water-Wastewater-Utilities/dp/1572784717


A GUIDE TO CYBERSECURITY FOR WATER AND WASTEWATER UTILITIES
By Steve Mustard, PE, CAP, GICSP
Water Environment Federation
the water quality people

ICS security news selection

US lawmakers propose legislation to expand cyber threat coordination across energy sector

Two U.S. Senators have introduced legislation designed to deepen cybersecurity collaboration within the nation's energy infrastructure. The proposed measure seeks to formalize and expand the role of the Department of Energy's Energy Threat Analysis Center in facilitating cross-sector threat intelligence exchange.

Titled 'Energy Threat Analysis Program Act,' the bipartisan legislative effort if enacted would authorize the Center to serve as a strategic conduit for cyber threat assessments and mitigation strategies, coordinating efforts among the Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the intelligence community, and private-sector energy operators. …

Source and more information:

https://industrialcyber.co/regulation-standards-and-compliance/us-lawmakers-propose-legislation-to-expand-cyber-threat-coordination-across-energy-sector/

Ransomware and USB attacks are hammering OT systems

Ransomware, trojans, and malware delivered through USB devices are putting growing pressure on industrial systems, according to the Honeywell 2025 Cyber Threat Report, which draws on data from monitoring tools deployed across industrial sites around the world. The findings highlight persistent and serious risks to OT environments that keep critical infrastructure running.

Researchers recorded a 46 percent increase in ransomware extortion cases in late 2024 and early 2025. The Cl0p ransomware group was especially active. In just the first quarter of 2025, Honeywell tracked 2,472 ransomware victims globally, adding to the 6,130 incidents recorded in 2024. …

Source and more information:

https://www.helpnetsecurity.com/2025/06/06/honeywell-2025-cyber-threat-report/

OT remote access security: Building resilient, risk-aware access in industrial environments

Remote access across operational technology (OT) is under more strain than ever before. Vulnerabilities in legacy systems that cyber adversaries are increasingly exploiting with alarming precision are growing alongside industrial networks. Convenience-driven traditional OT remote access security solutions frequently fall victim to complex attacks, exposing vital infrastructure. It's just as hard not to let operational defenses get in the way of organizational agility.

Balancing usability with security is walking a tightrope. Lax rules breed violations, but overly strict rules can hinder productivity. Granular access restrictions, adaptive authentication, and session monitoring that adapts to risk, without getting in the way of workflows, are the answer. …

Source and more information:

https://industrialcyber.co/features/ot-environments-must-bake-security-into-remote-access-as-organizations-shift-toward-risk-aware-model/

APT-C-36 Hackers Attacking Government Institutions, Financial Organizations, and Critical Infrastructure

Since 2018, the advanced persistent threat group APT-C-36, commonly known as Blind Eagle, has emerged as a formidable cyber adversary targeting critical sectors across Latin America.

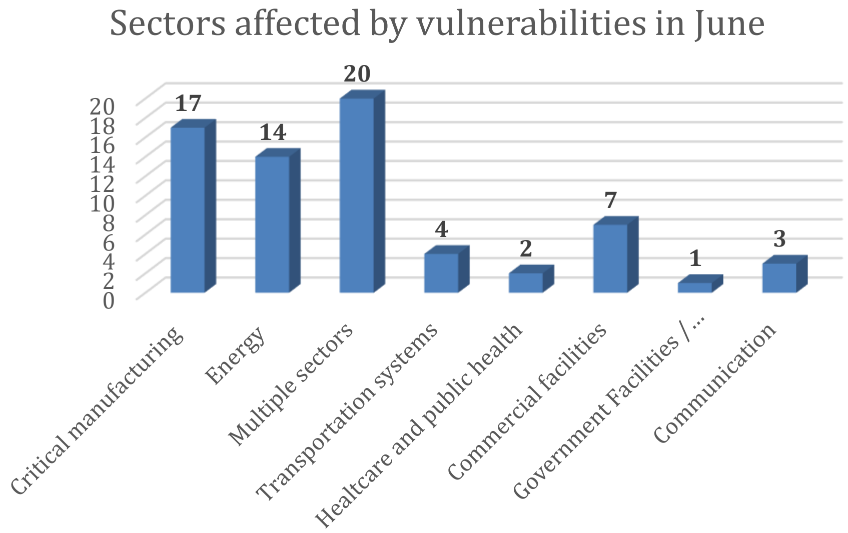
This sophisticated threat actor has demonstrated persistent focus on Colombian organizations, launching coordinated attacks against government institutions, financial organizations, and critical infrastructure through carefully orchestrated phishing campaigns and deployment of Remote Access Trojans (RATs). …

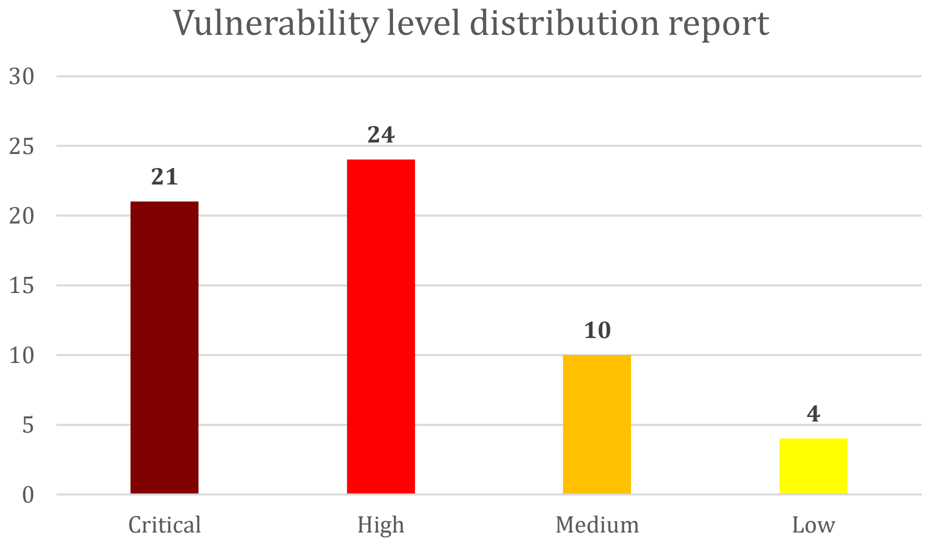
Source and more information:

https://cybersecuritynews.com/apt-c-36-hackers-attacking-government-institutions/

ICS vulnerabilities

In June 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-25-177-01: **Mitsubishi Electric Air Conditioning Systems**

Critical level vulnerability: Missing Authentication for Critical Function.

Mitsubishi Electric Air Conditioning Systems | CISA

ICSA-25-177-02: **TrendMakers Sight Bulb Pro**

Medium level vulnerabilities: Use of a Broken or Risky Cryptographic Algorithm, Improper Neutralization of Special Elements used in a Command ('Command Injection').

TrendMakers Sight Bulb Pro | CISA

ICSA-25-175-01: **Kaleris Navis N4 Terminal Operating System**

Critical level vulnerabilities: Deserialization of Untrusted Data, Cleartext Transmission of Sensitive Information.

Kaleris Navis N4 Terminal Operating System | CISA

ICSA-25-175-02: **Delta Electronics CNCSoft**

High level vulnerability: Out-of-bounds Write.

Delta Electronics CNCSoft | CISA

ICSA-25-175-03: **Schneider Electric Modicon Controllers**

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

Schneider Electric Modicon Controllers | CISA

ICSA-25-175-04: **Schneider Electric EVLink WallBox**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Schneider Electric EVLink WallBox | CISA

ICSA-25-175-05: **ControlID iDSecure On-Premises**

Critical level vulnerabilities: Improper Authentication, Server-Side Request Forgery (SSRF), SQL Injection.

ControlID iDSecure On-Premises | CISA

ICSA-25-175-06: **Parsons AccuWeather Widget**

High level vulnerability: Cross-site Scripting.

Parsons AccuWeather Widget | CISA

ICSA-25-175-07: **MICROSENS NMP Web+**

Critical level vulnerabilities: Use of Hard-coded, Security-relevant Constants, Insufficient Session Expiration, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

MICROSENS NMP Web+ | CISA

ICSA-19-029-02: **Mitsubishi Electric MELSEC-Q Series PLCs (Update B)**

High level vulnerability: Resource Exhaustion.

Mitsubishi Electric MELSEC-Q Series PLCs (Update B) | CISA

ICSA-25-168-01: **Siemens Mendix Studio Pro**

Low level vulnerability: Path Traversal.

Siemens Mendix Studio Pro | CISA

ICSA-25-168-02: **LS Electric GMWin 4**

High level vulnerabilities: Out-of-Bounds Write, Out-of-Bounds Read, Heap-based Buffer Overflow.

LS Electric GMWin 4 | CISA

ICSA-25-168-04: **Fuji Electric Smart Editor**

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

Fuji Electric Smart Editor | CISA

ICSA-25-168-05: **Dover Fueling Solutions ProGauge MagLink LX Consoles**

Critical level vulnerability: Missing Authentication for Critical Function.

Dover Fueling Solutions ProGauge MagLink LX Consoles | CISA

ICSA-24-347-10: **Siemens SENTRON Powercenter 1000 (Update A)**

High level vulnerability: Incorrect Synchronization.

Siemens SENTRON Powercenter 1000 (Update A) | CISA

SSA-726617: **Siemens Mendix OIDC SSO Module** **(Update: 1.2.)**

Low level vulnerability: Incorrect Privilege Assignment.

SSA-726617

SSA-928984: **Siemens User Management Component (UMC)** **(Update: 1.3.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-928984

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs** **(Update: 1.7.)**

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

SSA-876787

SSA-874353: **Siemens Mendix Runtime** **(Update: 1.3.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-874353

SSA-858251: **Siemens OPC UA** **(Update: 1.1.)**

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

SSA-858251

SSA-770770: **Fortigate NGFW Before V7.4.7 on Siemens RUGGEDCOM APE1808 Devices** **(Update: 1.4.)**

Critical level vulnerabilities: Multiple.

SSA-770770

SSA-698820: **Fortigate NGFW Before V7.4.4 on Siemens RUGGEDCOM APE1808 Devices** **(Update: 1.3.)**

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, Buffer Over-read.

SSA-698820

SSA-656895: **Siemens Teamcenter** **(Update: 1.3.)**

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

SSA-656895

SSA-620799: **Siemens SENTRON Powercenter 1000/1100 (Update: 1.1.)**

High level vulnerability: Incorrect Synchronization.

SSA-620799

SSA-497656: **Siemens TIM 4R-IE Devices (Update: 1.1.)**

Critical level vulnerabilities: Incorrect Conversion between Numeric Types, Improper Input Validation, Improper Authentication, Authentication Bypass by Capture-replay, NULL Pointer Dereference, Incorrect Synchronization, Authentication Bypass by Spoofing, Exposure of Sensitive Information to an Unauthorized Actor, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

SSA-497656

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP >= V3.1.0 and < V3.1.5 (Update: 2.6.)**

Critical level vulnerabilities: Multiple.

SSA-398330

SSA-366067: **Fortigate NGFW Before V7.4.1 on Siemens RUGGEDCOM APE1808 Devices (Update: 1.4.)**

Critical level vulnerabilities: Multiple.

SSA-366067

SSA-354569: **Palo Alto Networks PAN-OS on Siemens RUGGEDCOM APE1808 Devices (Update: 1.5.)**

Critical level vulnerabilities: Multiple.

SSA-354569

SSA-340240: **Siemens SIRIUS 3RV2921-5M (Update: 1.2.)**

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

SSA-340240

SSA-301229: **Siemens RUGGEDCOM ROX II (Update: 1.1.)**

Critical level vulnerability: Client-Side Enforcement of Server-Side Security.

SSA-301229

SSA-265688: **Siemens SIMATIC S7-1500 TM MFP V1.1 (Update: 1.6.)**

Critical level vulnerabilities: Multiple.

SSA-265688

SSA-216014: **Siemens SIMATIC IPCs, SIMATIC Tablet PCs, and SIMATIC Field PGs (Update: 1.1.)**

High level vulnerability: Protection Mechanism Failure.

SSA-216014

SSA-162506: **Siemens SIMOTICS CONNECT 400, Desigo PXC/PXM, APOGEE MEC/MBC/PXC, APOGEE PXC Series, and TALON TC Series (Update: 1.4.)**

High level vulnerability: Improper Input Validation.

SSA-162506

SSA-054046: **Siemens SIMATIC S7-1500 CPUs (Update: 1.6.)**

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

SSA-054046

ICSA-25-162-01: **Siemens Tecnomatix Plant Simulation**

High level vulnerability: Out-of-bounds Read.

Siemens Tecnomatix Plant Simulation | CISA

ICSA-25-162-02: **Siemens RUGGEDCOM APE1808**

Medium level vulnerability: Cross-site Scripting.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-25-162-03: **Siemens SCALANCE and RUGGEDCOM**

Medium level vulnerability: Improper Privilege Management.

Siemens SCALANCE and RUGGEDCOM | CISA

ICSA-25-162-04: **Siemens SCALANCE and RUGGEDCOM**

High level vulnerabilities: Incorrect Authorization, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

Siemens SCALANCE and RUGGEDCOM | CISA

ICSA-25-162-05: **Siemens SIMATIC S7-1500 CPU Family**

High level vulnerabilities: Missing Encryption of Sensitive Data, Out-of-bounds Read, Use After Free, Stack-based Buffer Overflow, Incorrect Provision of Specified Functionality, Out-of-bounds Write, Incorrect Calculation of Buffer Size, Heap-based Buffer Overflow, External Control of File Name or Path, Uncontrolled Resource Consumption, Improper Input Validation, Truncation of Security-relevant Information, Missing Critical Step in Authentication, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Access of Resource Using Incompatible Type ('Type Confusion'), Signal Handler Race Condition, Inefficient Algorithmic Complexity, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), NULL Pointer Dereference, Reachable Assertion, Return of Pointer Value Outside of Expected Range, Improper Handling of Length Parameter Inconsistency, Integer Overflow or Wraparound, Improper Locking, Improper Validation of Array Index, Buffer Underwrite ('Buffer Underflow'), Use of Uninitialized Resource, Detection of Error Condition Without Action, Premature Release of Resource During Expected Lifetime.

Siemens SIMATIC S7-1500 CPU Family | CISA

ICSA-25-162-06: **Siemens Energy Services**

Critical level vulnerability: Incorrect Default Permissions.

Siemens Energy Services | CISA

ICSA-25-162-07: **AVEVA PI Data Archive**

High level vulnerabilities: Uncaught Exception, Heap-based Buffer Overflow.

AVEVA PI Data Archive | CISA

ICSA-25-162-08: **AVEVA PI Web API**

Low level vulnerability: Cross-site Scripting.

AVEVA PI Web API | CISA

ICSA-25-162-09: **AVEVA PI Connector for CygNet**

Medium level vulnerabilities: Cross-site Scripting, Improper Validation of Integrity Check Value.

AVEVA PI Connector for CygNet | CISA

ICSA-25-162-10: **PTZOptics and Other Pan-Tilt-Zoom Cameras**

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

PTZOptics and Other Pan-Tilt-Zoom Cameras | CISA

ICSA-25-160-01: **SinoTrack GPS Receiver**

High level vulnerabilities: Weak Authentication, Observable Response Discrepency.

SinoTrack GPS Receiver | CISA

ICSA-25-160-02: **Hitachi Energy Relion 670, 650, SAM600-IO Series**

High level vulnerability: Observable Discrepancy.

Hitachi Energy Relion 670, 650, SAM600-IO Series | CISA

ICSMA-25-160-01: **MicroDicom DICOM Viewer**

High level vulnerability: Out-of-bounds Write.

MicroDicom DICOM Viewer | CISA

ICSA-25-140-11: **Assured Telematics Inc (ATI) Fleet Management System (Update A)** **High** level vulnerability: Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Assured Telematics Inc (ATI) Fleet Management System (Update A) | CISA

ICSA-25-155-01: **CyberData 011209 SIP Emergency Intercom**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Missing Authentication for Critical Function, SQL Injection, Insufficiently Protected Credentials, Path Traversal: '.../...//'.

CyberData 011209 SIP Emergency Intercom | CISA

ICSA-25-155-02: **Hitachi Energy Relion 670, 650 series and SAM600-IO Product**

Critical level vulnerability: Integer Overflow or Wraparound.

Hitachi Energy Relion 670, 650 Series and SAM600-IO Product | CISA

ICSA-21-049-02: **Mitsubishi Electric FA Engineering Software Products (Update H)**

High level vulnerabilities: Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency.

Mitsubishi Electric FA Engineering Software Products (Update H) | CISA

ICSA-25-133-02: **Hitachi Energy Relion 670/650/SAM600-IO Series (Update A)**

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

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

ICSA-23-068-05: **Hitachi Energy Relion 670, 650 and SAM600-IO Series (Update A)** **Medium** level vulnerability: Insufficient Verification of Data Authenticity.

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

ICSA-21-336-05: **Hitachi Energy Relion 670/650/SAM600-IO (Update A)**

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

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

ICSA-23-089-01: **Hitachi Energy IEC 61850 MMS-Server (Update A)**

Medium level vulnerability: Improper Resource Shutdown or Release.

Hitachi Energy IEC 61850 MMS-Server (Update A) | CISA

ICSA-25-153-01: **Schneider Electric Wiser Home Automation**

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

Schneider Electric Wiser Home Automation | CISA

ICSA-25-153-02: **Schneider Electric EcoStruxure Power Build Rapsody**

Low level vulnerability: Stack-based Buffer Overflow.

Schneider Electric EcoStruxure Power Build Rapsody | CISA

ICSA-25-153-03: **Mitsubishi Electric MELSEC iQ-F Series**

Critical level vulnerability: Improper Validation of Specified Index, Position, or Offset in Input.

Mitsubishi Electric MELSEC iQ-F Series | 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 June:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2021-32030 ASUS Routers Improper Authentication Vulnerability;
CVE-2023-39780 ASUS RT-AX55 Routers OS Command Injection Vulnerability;
CVE-2024-56145 Craft CMS Code Injection Vulnerability;
CVE-2025-3935 ConnectWise ScreenConnect Improper Authentication Vulnerability;
CVE-2025-35939 Craft CMS External Control of Assumed-Immutable Web Parameter Vulnerability;
CVE-2025-21479 Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability;
CVE-2025-21480 Qualcomm Multiple Chipsets Incorrect Authorization Vulnerability;
CVE-2025-27038 Qualcomm Multiple Chipsets Use-After-Free Vulnerability;
CVE-2025-5419 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability;
CVE-2025-32433 Erlang Erlang/OTP SSH Server Missing Authentication for Critical Function Vulnerability;
CVE-2024-42009 RoundCube Webmail Cross-Site Scripting Vulnerability;
CVE-2025-24016 Wazuh Server Deserialization of Untrusted Data Vulnerability;
CVE-2025-33053 Web Distributed Authoring and Versioning (WebDAV) External Control of File Name or Path Vulnerability;
CVE-2025-43200 Apple Multiple Products Unspecified Vulnerability;
CVE-2023-33538 TP-Link Multiple Routers Command Injection Vulnerability;
CVE-2023-0386 Linux Kernel Improper Ownership Management Vulnerability;
CVE-2024-54085 AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability;
CVE-2024-0769 D-Link DIR-859 Router Path Traversal Vulnerability;
CVE-2019-6693 Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability;
CVE-2025-6543 Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability;
Links and more information:
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds 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 One Known Exploited Vulnerability to Catalog | CISA

Updated Guidance on Play Ransomware
CISA, the Federal Bureau of Investigation (FBI), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) have issued an updated advisory on Play ransomware, also known as Playcrypt. This advisory highlights new tactics, techniques,

and procedures used by the Play ransomware group and provides updated indicators of compromise (IOCs) to enhance threat detection.
Links and more information:
[Updated Guidance on Play Ransomware | CISA]

CISA Releases Cybersecurity Advisory on SimpleHelp RMM Vulnerability
CISA released Cybersecurity Advisory: Ransomware Actors Exploit Unpatched SimpleHelp Remote Monitoring and Management to Compromise Utility Billing Software Provider. This advisory is in response to ransomware actors targeting customers of a utility billing software provider through unpatched vulnerabilities in SimpleHelp Remote Monitoring and Management (RMM).
Links and more information:
[CISA Releases Cybersecurity Advisory on SimpleHelp RMM Vulnerability | CISA]

New Guidance Released for Reducing Memory-Related Vulnerabilities
CISA, in partnership with the National Security Agency (NSA), released a joint guide on reducing memory-related vulnerabilities in modern software development.
Memory safety vulnerabilities pose serious risks to national security and critical infrastructure. Adopting memory safe languages (MSLs) offers the most comprehensive mitigation against this class of vulnerabilities and provides built-in safeguards that enhance security by design.
Links and more information:
[New Guidance Released for Reducing Memory-Related Vulnerabilities | CISA]

CISA and Partners Urge Critical Infrastructure to Stay Vigilant in the Current Geopolitical Environment
CISA, in collaboration with the Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA), released a Fact Sheet urging organizations to remain vigilant against potential targeted cyber operations by Iranian state-sponsored or affiliated threat actors.
Links and more information:
[CISA and Partners Urge Critical Infrastructure to Stay Vigilant in the Current Geopolitical Environment | CISA]

ICS trainings, education

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