2025 July, 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 2
ICS conferences 3
ICS incidents 5
Book recommendation 9
ICS security news selection 10
ICS vulnerabilities 12
ICS alerts 24
ICS trainings, education 28
ICS podcasts 31

ICS good practices, recommendations

Best Practices and Strategies for Effective Factory Security

Ensuring robust factory security measures is paramount in today's rapidly evolving industrial landscape. Whether you manage a small manufacturing facility or oversee a large production plant, safeguarding your assets, employees, and sensitive information is crucial. Let's delve into some best practices and strategies to enhance factory security:

1. Risk Assessment and Threat Modeling
2. Access Control and Surveillance
3. Personnel Training and Awareness
4. Physical Security Measures
5. Cybersecurity
6. Emergency Preparedness
7. Collaboration with Security Providers

conclusion

Effective factory security requires a multifaceted approach. By implementing these best practices, you'll create a safer environment for your workforce and protect valuable assets. Security is ongoing, so stay vigilant and adapt to changing threats. And when considering professional security services, trust American Global Security to keep your factory secure around the clock.

Source and more detailed information (about the 7 points) available on the following link:

https://americanglobalsecurity.com/best-practices-and-strategies-for-effective-factory-security/

ICS conferences

In August 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 19th August 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, 19th August 2025

More details can be found on the following website:

https://otsecsummit.com/#

Dragos APAC Inaugural Partner Summit

This complimentary event offers the opportunity to engage, exchange, and experience the difference Dragos and partners across the ecosystem within Asia Pacific and Japan are making, continuing to make, and forecasting across critical industries in the OT/ICS landscape.

Attendees can look forward to interacting with Dragos executives from the United States, who will offer insights into the current market landscape, future directions, and how to capitalise on regional opportunities. The event will include a series of information exchanges, operational technology workshops divided into an

executive/sales track and a technology (SE) track, showcasing how Dragos is evolving through product and technology innovations.

Additionally, there will be a networking event following the summit, providing a chance to connect and exchange insights with industry peers, including technology partners, OEM partners, and channel ecosystems.

Rivershed West, Howard Smith Wharves, Brisbane, Australia; 25th August 2025

More details can be found on the following website:

Dragos APAC Inaugural Partner Summit

ICS incidents

Major food wholesaler says cyberattack impacting distribution systems

On June 5, United Natural Foods (UNFI), one of the largest health and specialty food distributors in the U.S. and Canada, suffered a significant cyberattack that led to the shutdown of key systems and disrupted business operations. In filings with the U.S. Securities and Exchange Commission (SEC) and a public statement, the Rhode Island-based company confirmed it had detected unauthorized activity and took systems offline to contain the threat.

As a result, UNFI reported that its ability to fulfil and distribute customer orders was temporarily halted. The company acknowledged ongoing operational disruptions and emphasized that these interruptions are expected to persist in the near term. While workarounds have been implemented to maintain some level of service, full system restoration is still in progress.

UNFI has engaged a cybersecurity firm to investigate and remediate the incident and law enforcement has been notified. The investigation is still in its early stages.

UNFI is a key supplier to Whole Foods and reported $8.2 billion in net sales last quarter. This incident adds to a growing list of cyberattacks targeting the food and agriculture sector. Notable past victims include JBS (2021), Dole, Sysco, Mondelez, Americold, and Ahold Delhaize USA — the latter experiencing major outages across its 2,000+ stores just before Thanksgiving 2024.

These recurring attacks underscore the sector's vulnerability and the critical need for robust cybersecurity measures to protect supply chains and food distribution networks.

The source is available on the following link:

https://therecord.media/major-food-wholesaler-cyberattack-impacting-distribution

Canadian Electric Utility Says Power Meters Disrupted by Cyberattack

Nova Scotia Power, a Canadian electric utility, has confirmed that a recent cyberattack has disrupted communication between its smart meters and internal systems. While the meters continued to accurately record energy usage, the data could not be transmitted properly, which led the company to temporarily pause billing. Billing has since resumed, although many customers are currently receiving estimated invoices until full system functionality is restored.

The cyberattack, which occurred in April, was identified as a ransomware incident that resulted in the theft of sensitive customer data. Exposed information includes names, birthdates, contact details, energy usage data, and in some cases, highly sensitive identifiers such as Social Insurance Numbers, driver's license numbers, and bank account details.

Nova Scotia Power has not disclosed which ransomware group is responsible for the breach, and no known threat actor has publicly claimed responsibility. The breach has impacted approximately 280,000 out of 550,000 customers, and former customers are also affected.

Although Nova Scotia Power does not operate in the United States directly, its parent company, Emera, provides utility services across North America. So far, 377 residents of Maine have been confirmed among the affected individuals, but the total number of impacted U.S. residents remains unclear.

The utility continues its investigation and is notifying affected individuals, including those in the United States, about the breach and potential data exposure.

The source is available on the following link:

https://www.securityweek.com/canadian-electric-utility-says-power-meters-disrupted-by-cyberattack/

Book recommendation

Industrial Cybersecurity and Operational Technology Security (OT)

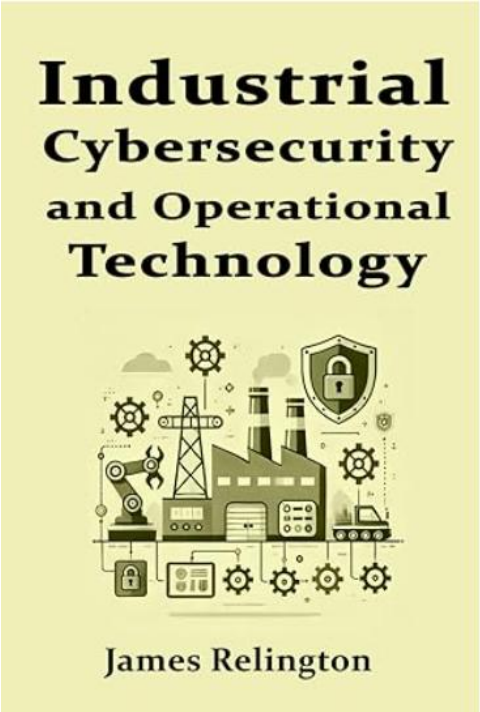
This book explores cybersecurity in industrial and operational technology (OT) environments in depth, addressing the challenges, threats, and protection strategies in critical infrastructures. From identifying vulnerabilities to implementing advanced security models, it analyzes real cases of cyberattacks, key regulations, and emerging trends in the protection of industrial control systems. With a practical and strategic approach, it offers essential recommendations to strengthen the resilience of organizations to the growing cyber threats in an increasingly digitalized and interconnected world.

Author/Editor: James Relington (Author)

Year of issue: 2025

The book is available at the following link:

https://www.amazon.com/Industrial-Cybersecurity-Operational-Technology-Security/dp/B0DXQ1GBQ8



ICS security news selection

Industrial security is on shaky ground and leaders need to pay attention

44% of industrial organizations claim to have strong real-time cyber visibility, but nearly 60% have low to no confidence in their OT and IoT threat detection capabilities, according to Forescout.

Digitalization raises industrial cyber risks

Digitalization has increased connectivity across devices, transforming industrial environments, which in turn increases cyber risk. Rising geopolitical tensions further compound these challenges, demanding more nuanced, strategic and integrated security approaches to protect critical assets while maintaining operations. …

Source and more information:

https://www.helpnetsecurity.com/2025/07/03/ot-iot-threat-detection-confidence/

Iranian Hackers' Preferred ICS Targets Left Open Amid Fresh US Attack Warning

Several US government agencies on Monday issued a fresh warning over Iranian threat actors targeting critical infrastructure, and researchers caution that many instances of these hackers' preferred targets remain exposed on the internet.

The Department of Homeland Security warned on June 22 that Iran is likely to retaliate — both in the real world and in cyberspace — after the United States conducted air strikes on three important nuclear sites in Iran.

Iranian and pro-Iran threat actors could conduct a wide range of attacks, including ransomware attacks, DDoS attacks, phishing, brute force attacks, and espionage. However, one primary concern is related to Iran's attacks on industrial control systems (ICS) and other operational technology (OT). …

Source and more information:

https://www.securityweek.com/iranian-hackers-preferred-ics-targets-left-open-amid-fresh-us-attack-warning/

Fortinet finds OT security maturity reduces attacks, as more CISOs are at the helm in 2025

Fortinet revealed persistent gaps, pointing to critical areas where organizations must strengthen their defenses as IT and OT (operational technology) environments become increasingly interconnected and exposed. In 2025, 52% of organizations now place OT security under the CISO, up from just 16% in 2022. With 80% planning to follow their lead, CISOs are expanding security operations, automation, and threat intelligence into OT environments, bringing industrial cybersecurity into boardroom focus, as responsibility for OT security continues to elevate within executive ranks. …

Source and more information:

https://industrialcyber.co/reports/fortinet-finds-ot-security-maturity-reduces-attacks-as-more-cisos-are-at-the-helm-in-2025/

Critical cyber flaw linked to EoT module ignored in US rail systems for 12 years, fix not expected until 2027

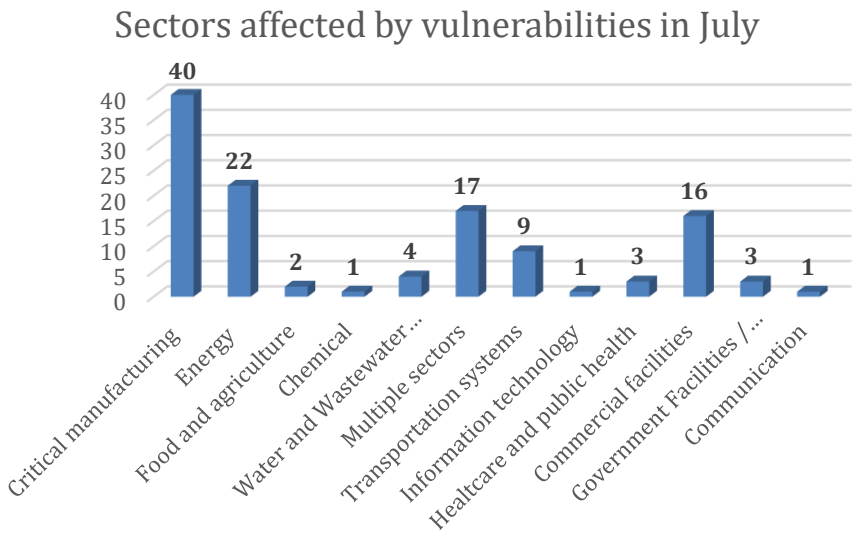
A critical cybersecurity vulnerability affecting American train systems has gone unaddressed for over a decade, despite early warnings dating back to 2012. The issue, tied to End-of-Train (EoT) modules that transmit telemetry data wirelessly from the rear to the front of freight trains, was first identified by hardware security researcher Neils in 2012. He shared details last week on X, formerly Twitter, noting the risk emerged when software-defined radios (SDRs) became more accessible, allowing attackers to potentially intercept or spoof EoT communications. …

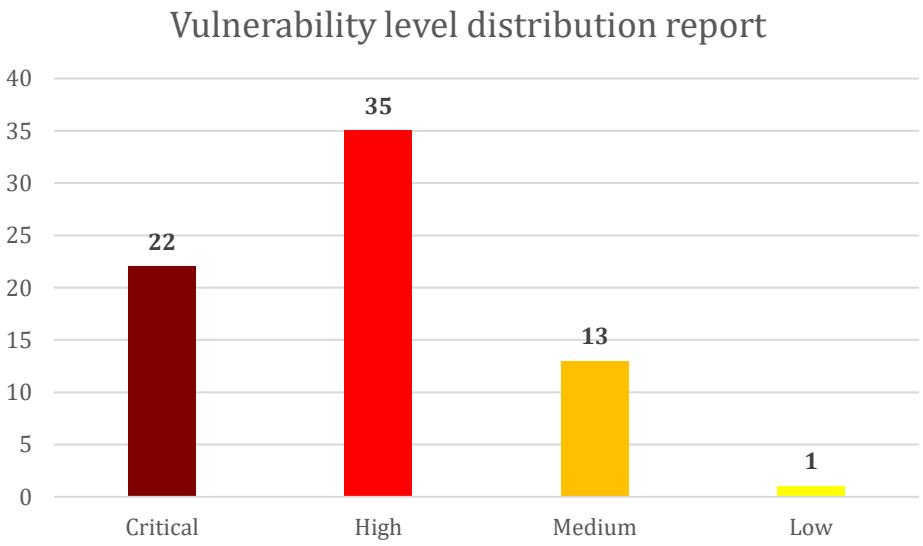
Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/critical-cyber-flaw-linked-to-eot-module-ignored-in-us-rail-systems-for-12-years-fix-not-expected-until-2027/

ICS vulnerabilities

In July 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-25-212-01: **Güralp FMUS Series Seismic Monitoring Devices**

Critical level vulnerability: Missing Authentication for Critical Function.

Güralp Systems Güralp FMUS series | CISA

ICSA-25-212-02: **Rockwell Automation Lifecycle Services with VMware**

Critical level vulnerabilities: Out-of-bounds Write, Use of Uninitialized Resource.

Rockwell Automation Lifecycle Services with VMware | CISA

ICSA-24-158-04: **Johnson Controls Software House iStar Pro Door Controller (Update A)**

High level vulnerability: Missing Authentication for Critical Function.

Johnson Controls Software House iStar Door Controller (Update A) | CISA

ICSA-24-338-06: **Fuji Electric Tellus Lite V-Simulator (Update A)**

High level vulnerability: Out-of-bounds Write.

Fuji Electric Tellus Lite V-Simulator (Update A) | CISA

ICSA-25-210-01: **National Instruments LabVIEW**

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

National Instruments LabVIEW | CISA

ICSA-25-210-02: **Samsung HVAC DMS**

High level vulnerabilities: Execution After Redirect (EAR), Deserialization of Untrusted Data, Absolute Path Traversal, Use of Potentially Dangerous Function, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Relative Path Traversal.

Samsung HVAC DMS | CISA

ICSA-25-210-03: **Delta Electronics DTN Soft**

High level vulnerability: Deserialization of Untrusted Data.

Delta Electronics DTN Soft | CISA

ICSA-25-205-01: **Mitsubishi Electric CNC Series**

High level vulnerability: Uncontrolled Search Path Element.

Mitsubishi Electric CNC Series | CISA

ICSA-25-205-02: **Network Thermostat X-Series WiFi Thermostats**

Critical level vulnerability: Missing Authentication for Critical Function.

Network Thermostat X-Series WiFi Thermostats | CISA

ICSA-25-205-03: **Honeywell Experion PKS**

Critical level vulnerabilities: Use of Uninitialized Variable, Improper Restriction of Operations within the Bounds of a Memory Buffer, Sensitive Information in Resource Not Removed Before Reuse, Integer Underflow (Wrap or Wraparound), Deployment of Wrong Handler.

Honeywell Experion PKS | CISA

ICSA-25-205-04: **LG Innotek Camera Model LNV5110R**

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

LG Innotek Camera Model LNV5110R | CISA

ICSMA-25-205-01: **Medtronic MyCareLink Patient Monitor**

High level vulnerabilities: Cleartext Storage of Sensitive Information, Empty Password in Configuration File, Deserialization of Untrusted Data.

Medtronic MyCareLink Patient Monitor | CISA

ICSA-22-202-04: **ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update A)**

Critical level vulnerabilities: Path Traversal, Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere, Out-of-Bounds Read.

ICONICS Suite and Mitsubishi Electric MC Works64 Products (Update A) | CISA

ICSA-25-203-01: **DuraComm DP-10iN-100-MU**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Missing Authentication for a Critical Function, Improper Neutralization of Input During Web Page Generation.

DuraComm DP-10iN-100-MU | CISA

ICSA-25-203-02: **Lantronix Provisioning Manager**

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

Lantronix Provisioning Manager | CISA

ICSA-25-203-03: **Schneider Electric EcoStruxure**

Medium level vulnerability: Exposure of Resource to Wrong Sphere.

Schneider Electric EcoStruxure | CISA

ICSA-25-203-04: **Schneider Electric EcoStruxure Power Operation**

High level vulnerabilities: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'), Integer Overflow to Buffer Overflow, Improper Handling of Highly Compressed Data (Data Amplification), Out-of-bounds Write, Uncontrolled Resource Consumption.

Schneider Electric EcoStruxure Power Operation | CISA

ICSA-25-203-05: **Schneider Electric System Monitor Application**

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

Schneider Electric System Monitor Application | CISA

ICSA-25-203-06: **Schneider Electric EcoStruxture IT Data Center Expert**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Insufficient Entropy, Improper Control of Generation of Code ('Code Injection'), Server-Side Request Forgery (SSRF), Improper Privilege Management, and Improper Restriction of XML External Entity Reference.

Schneider Electric EcoStruxture IT Data Center Expert | CISA

ICSA-25-175-03: **Schneider Electric Modicon Controllers (Update A)**

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

Schneider Electric Modicon Controllers (Update A) | CISA

ICSA-25-175-04: **Schneider Electric EVLink WallBox (Update A)**

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 (Update A) | CISA

ICSA-25-014-02: **Schneider Electric Vijeo Designer (Update A)**

High level vulnerability: Improper Privilege Management.

Schneider Electric Vijeo Designer and EcoStruxure Machine Expert (Update A) | CISA

ICSA-25-198-01: **Leviton AcquiSuite and Energy Monitoring Hub**

High level vulnerability: Cross-site Scripting.

Leviton AcquiSuite and Energy Monitoring Hub | CISA

ICSMA-25-198-01: **Panoramic Corporation Digital Imaging Software**

High level vulnerability: Uncontrolled Search Path Element.

Panoramic Corporation Digital Imaging Software | CISA

ICSA-24-191-05: **Johnson Controls Inc. Software House C●CURE 9000 (Update B)**

High level vulnerability: Incorrect Default Permissions.

Johnson Controls Software House C●CURE 9000 (Update B) | CISA

ICSA-25-196-01: **Hitachi Energy Asset Suite**

Critical level vulnerabilities: Incomplete List of Disallowed Inputs, Plaintext Storage of a Password, Out-of-bounds Write, Release of Invalid Pointer or Reference.

Hitachi Energy Asset Suite | CISA

ICSA-25-196-02: **ABB RMC-100**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Stack-based Buffer Overflow.

ABB RMC-100 | CISA

ICSA-25-196-03: **LITEON IC48A and IC80A EV Chargers**

High level vulnerability: Plaintext Storage of a Password.

LITEON IC48A and IC80A EV Chargers | CISA

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

High level vulnerability: Uncontrolled Search Path Element.

Schneider Electric EcoStruxure (Update B) | CISA

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

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

Schneider Electric Modicon Controllers (Update A) | CISA

ICSA-25-070-01: **Schneider Electric Uni-Telway Driver (Update A)**

Medium level vulnerability: Improper Input Validation.

Schneider Electric Uni-Telway Driver (Update A) | CISA

ICSA-25-191-01: **Siemens SINEC NMS**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Missing Authentication for Critical Function, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Siemens SINEC NMS | CISA

ICSA-25-191-02: **Siemens Solid Edge**

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

Siemens Solid Edge | CISA

ICSA-25-191-03: **Siemens TIA Administrator**

High level vulnerabilities: Improper Verification of Cryptographic Signature, Improper Access Control.

Siemens TIA Administrator | CISA

ICSA-25-191-04: **Siemens SIMATIC CN 4100**

High level vulnerability: Improper Input Validation.

Siemens SIMATIC CN 4100 | CISA

ICSA-25-191-05: **Siemens TIA Project-Server and TIA Portal**

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

Siemens TIA Project-Server and TIA Portal | CISA

ICSA-25-191-06: **Siemens SIPROTEC 5**

Medium level vulnerability: Use of GET Request Method With Sensitive Query Strings.

Siemens SIPROTEC 5 | CISA

ICSA-25-191-07: **Delta Electronics DTM Soft**

High level vulnerability: Deserialization of Untrusted Data.

Delta Electronics DTM Soft | CISA

ICSA-25-191-08: **Advantech iView**

High level vulnerabilities: Cross-site Scripting, SQL Injection, Path Traversal, Argument Injection.

Advantech iView | CISA

ICSA-25-191-09: **KUNBUS RevPi Webstatus**

Critical level vulnerability: Incorrect Implementation of Authentication Algorithm.

KUNBUS RevPi Webstatus | CISA

ICSA-25-191-10: **End-of-Train and Head-of-Train Remote Linking Protocol**

High level vulnerability: Weak Authentication.

End-of-Train and Head-of-Train Remote Linking Protocol | CISA

ICSA-25-121-01: **KUNBUS GmbH Revolution Pi (Update A)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Authentication Bypass by Primary Weakness, Improper Neutralization of Server-Side Includes (SSI) Within a Web Page.

KUNBUS GmbH Revolution Pi (Update A) | CISA

ICSA-25-135-19: **ECOVACS DEEBOT Vacuum and Base Station (Update A)**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Download of Code Without Integrity Check.

ECOVACS DEEBOT Vacuum and Base Station (Update A) | CISA

ICSA-24-263-02: **IDEC Products (Update A)**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Generation of Predictable Identifiers.

IDEC Products (Update A) | CISA

SSA-876787: **Open Redirect Vulnerability in SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.8.)**

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

SSA-876787

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

Medium level vulnerabilities: Insufficiently Protected Credentials, Insufficient Session Expiration, Out-of-bounds Write, Authentication Bypass Using an Alternate Path or Channel, Improper Certificate Validation, Exposure of Sensitive Information to an Unauthorized Actor.

SSA-864900

SSA-770770: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.7 on RUGGEDCOM APE1808 Devices (Update: 1.5.)**

Critical level vulnerabilities: Multiple.

SSA-770770

SSA-763427: **Authentication Bypass Vulnerability in SIMATIC CP and TIM Devices (Update: 1.6.)**

Critical level vulnerability: Missing Authentication for Critical Function.

SSA-763427

SSA-725549: **Denial of Service of ICMP in Industrial Devices (Update: 1.1.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-725549

SSA-723487: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products (Update: 1.7.)**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-698820: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.4 on RUGGEDCOM APE1808 Devices (Update: 1.8.)**

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, Channel Accessible by Non-Endpoint, Buffer Over-read.

SSA-698820

SSA-634640: **Weak Authentication Vulnerability in Siemens Industrial Edge Devices (Update: 1.1.)**

Critical level vulnerability: Weak Authentication.

SSA-634640

SSA-627195: **Zip Path Traversal Vulnerability in Mendix Studio Pro's Module Installation Process (Update: 1.1.)**

Low level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

SSA-627195

SSA-614723: **Denial of Service Vulnerabilities in User Management Component (UMC) (Update: 1.1.)**

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

SSA-614723

SSA-593272: **SegmentSmack in Interniche IP-Stack based Industrial Devices (Update: 2.5.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-593272

SSA-513708: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Exposure of Sensitive System Information to an Unauthorized Control Sphere, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

SSA-513708

SSA-446545: **Impact of RegreSSHion (CVE-2024-6387) in Siemens Industrial Products (Update: 1.1.)**

High level vulnerability: Signal Handler Race Condition.

SSA-446545

SSA-366067: **Multiple Vulnerabilities in Fortigate NGFW Before V7.4.1 on RUGGEDCOM APE1808 Devices (Update: 1.5.)**

Critical level vulnerabilities: Multiple.

SSA-366067

SSA-364175: **Multiple Vulnerabilities in Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update: 1.6.)**

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, Uncontrolled Resource Consumption, Improper Neutralization of Special Elements used in a Command ('Command Injection').

SSA-364175

SSA-327438: **Multiple Vulnerabilities in SCALANCE LPE9403 (Update: 1.1.)**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Path Traversal: '.../...//', Use of Uninitialized Variable, NULL Pointer Dereference, Out-of-bounds Read, Stack-based Buffer Overflow, Authentication Bypass Using an Alternate Path or Channel, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Cleartext Transmission of Sensitive Information.

SSA-327438

SSA-265688: **Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1 (Update: 1.7.)**

Medium level vulnerabilities: Multiple.

SSA-265688

ICSA-25-189-01: **Emerson ValveLink Products**

Critical level vulnerabilities: Cleartext Storage of Sensitive Information in Memory, Protection Mechanism Failure, Uncontrolled Search Path Element, Improper Input Validation.

Emerson ValveLink Products | CISA

ICSA-25-184-01: **Hitachi Energy Relion 670/650 and SAM600-IO Series**

Medium level vulnerability: Overly Restrictive Account Lockout Mechanism.

Mitsubishi Electric MELSEC iQ-F Series | CISA

ICSA-25-184-02: **Hitachi Energy MicroSCADA X SYS600**

High level vulnerabilities: Incorrect Default Permissions, External Control of File Name or Path, Improper Validation of Integrity Check Value, Exposure of Sensitive Information Through Data Queries, Improper Certificate Validation.

Hitachi Energy MicroSCADA X SYS600 | CISA

ICSA-25-184-03: **Mitsubishi Electric MELSOFT Update Manager**

High level vulnerabilities: Integer Underflow (Wrap or Wraparound), Protection Mechanism Failure.

Mitsubishi Electric MELSOFT Update Manager | CISA

ICSA-25-184-04: **Mitsubishi Electric MELSEC iQ-F Series**

Medium level vulnerability: Overly Restrictive Account Lockout Mechanism.

Mitsubishi Electric MELSEC iQ-F Series | CISA

ICSA-25-182-01: **FESTO Didactic CP, MPS 200, and MPS 400 Firmware**

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

FESTO Didactic CP, MPS 200, and MPS 400 Firmware | CISA

ICSA-25-182-02: **FESTO Automation Suite, FluidDraw, and Festo Didactic Products**

Critical level vulnerability: Out-of-bounds Write.

FESTO Automation Suite, FluidDraw, and Festo Didactic Products | CISA

ICSA-25-182-03: **FESTO CODESYS**

Critical level vulnerabilities: Partial String Comparison, Uncontrolled Resource Consumption, Memory Allocation with Excessive Size Value.

FESTO CODESYS | CISA

ICSA-25-182-04: **FESTO Hardware Controller, Hardware Servo Press Kit**

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

FESTO Hardware Controller, Hardware Servo Press Kit | CISA

ICSA-25-182-05: **Voltronic Power and PowerShield UPS Monitoring Software**

Critical level vulnerabilities: Exposed Dangerous Method or Function, Forced Browsing.

Voltronic Power and PowerShield UPS Monitoring Software | CISA

ICSA-25-182-06: **Hitachi Energy Relion 670/650 and SAM600-IO Series**

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

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

ICSA-25-182-07: **Hitachi Energy MSM**

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

Hitachi Energy MSM | 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-2025-48927 TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability;
CVE-2025-48928 TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability;
CVE-2025-6554 Google Chromium V8 Type Confusion Vulnerability;
CVE-2014-3931 Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability;
CVE-2016-10033 PHPMailer Command Injection Vulnerability;
CVE-2019-5418 Rails Ruby on Rails Path Traversal Vulnerability;
CVE-2019-9621 Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2025-5777 Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability;
CVE-2025-47812 Wing FTP Server Improper Neutralization of Null Byte or NUL Character Vulnerability;
CVE-2025-25257 Fortinet FortiWeb SQL Injection Vulnerability;
CVE-2025-53770: Microsoft SharePoint Server Remote Code Execution Vulnerability;
CVE-2025-54309 CrushFTP Unprotected Alternate Channel Vulnerability;
CVE-2025-6558 Google Chromium ANGLE and GPU Improper Input Validation Vulnerability;
CVE-2025-2776 SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability;
CVE-2025-2775 SysAid On-Prem Improper Restriction of XML External Entity Reference Vulnerability;
CVE-2025-49704 Microsoft SharePoint Code Injection Vulnerability;
CVE-2025-49706 Microsoft SharePoint Improper Authentication Vulnerability;
CVE-2025-20281 Cisco Identity Services Engine Injection Vulnerability;
CVE-2025-20337 Cisco Identity Services Engine Injection Vulnerability;
CVE-2023-2533 PaperCut NG/MF Cross-Site Request Forgery (CSRF) Vulnerability;
Links and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability, CVE-2025-53770 “ToolShell,” to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA

UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities

Update (07/31/2025): CISA has updated this alert to provide clarification on antivirus and endpoint detection and response (EDR) solutions, and details regarding mitigations related to the IIS server.
Update (07/24/2025): CISA continues to update reporting on this ongoing activity, as threat actor tactics, techniques, and procedures (TTPs) continue to evolve. This update contains additional information on the deployment of ransomware, new webshells involved in exploitation, and enhanced detection guidance.
Update (07/22/2025): This Alert was updated to reflect newly released information from Microsoft, and to correct the actively exploited Common Vulnerabilities and Exposures (CVEs), which have been confirmed as CVE-2025-49706, a network spoofing vulnerability, and CVE-2025-49704, a remote code execution (RCE) vulnerability.
Links and more information:
UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities | CISA

Joint Advisory Issued on Protecting Against Interlock Ransomware

CISA, in partnership with the Federal Bureau of Investigation (FBI), the Department of Health and Human Services, and the Multi-State Information Sharing and Analysis Center issued a joint Cybersecurity Advisory to help protect businesses and critical infrastructure organizations in North America and Europe against Interlock ransomware.
Links and more information:
Joint Advisory Issued on Protecting Against Interlock Ransomware | CISA

CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization

The Cybersecurity and Infrastructure Security Agency (CISA) and U.S. Coast Guard (USCG) are issuing this Cybersecurity Advisory to present findings from a recent CISA and USCG hunt engagement. The purpose of this advisory is to highlight identified cybersecurity issues, thereby informing security defenders in other organizations of potential similar issues and encouraging them to take proactive measures to enhance their cybersecurity posture. This advisory has been coordinated with the organization involved in the hunt engagement.
Links and more information:
CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization | CISA

CISA and Partners Release Updated Advisory on Scattered Spider Group

CISA, along with the Federal Bureau of Investigation, Canadian Centre for Cyber Security, Royal Canadian Mounted Police, the Australian Cyber Security Centre's Australian Signals Directorate, and the Australian Federal Police and National Cyber Security Centre, released an updated joint Cybersecurity Advisory on Scattered Spider—a cybercriminal group targeting commercial facilities sectors and subsectors. This advisory provides updated tactics, techniques, and procedures (TTPs) obtained through FBI investigations conducted through June 2025.

Scattered Spider threat actors have been known to use various ransomware variants in data extortion attacks, most recently including DragonForce ransomware. While Scattered Spider often changes TTPs to remain undetected, some TTPs remain consistent. These actors frequently use social engineering techniques such as phishing, push bombing, and subscriber identity module swap attacks to obtain credentials, install remote access tools, and bypass multi-factor authentication.

Links and more information:

CISA and Partners Release Updated Advisory on Scattered Spider Group | CISA

CISA Releases Part One of Zero Trust Microsegmentation Guidance

CISA released Microsegmentation in Zero Trust, Part One: Introduction and Planning as part of its ongoing efforts to support Federal Civilian Executive Branch (FCEB) agencies implementing zero trust architectures (ZTAs).

This guidance provides a high-level overview of microsegmentation, focusing on its key concepts, associated challenges and potential benefits, and includes recommended actions to modernize network security and advance zero trust principles.

Links and more information:

CISA Releases Part One of Zero Trust Microsegmentation Guidance | CISA

Eviction Strategies Tool Released

ISA released the Eviction Strategies Tool to provide cyber defenders with critical support and assistance during the containment and eviction phases of incident response. This tool includes:

- *Cyber Eviction Strategies Playbook Next Generation (Playbook-NG): A web-based application for next-generation operations.*
- *COUN7ER: A database of atomic post-compromise countermeasures users can execute based on adversary tactics, techniques, and procedures.*

Links and more information:

Eviction Strategies Tool Released | CISA

CISA and USCG Issue Joint Advisory to Strengthen Cyber Hygiene in Critical Infrastructure

CISA, in partnership with the U.S. Coast Guard (USCG), released a joint Cybersecurity Advisory aimed at helping critical infrastructure organizations improve their cyber

hygiene. This follows a proactive threat hunt engagement conducted at a U.S. critical infrastructure facility.
Links and more information:
CISA and USCG Issue Joint Advisory to Strengthen Cyber Hygiene in Critical Infrastructure | CISA

Thorium Platform Public Availability
CISA, in partnership with Sandia National Laboratories, announced the public availability of Thorium, a scalable and distributed platform for automated file analysis and result aggregation. Thorium enhances cybersecurity teams' capabilities by automating analysis workflows through seamless integration of commercial, open-source, and custom tools. It supports various mission functions, including software analysis, digital forensics, and incident response, allowing analysts to efficiently assess complex malware threats.
Links and more information:
Thorium Platform Public Availability | CISA

ICS trainings, education

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