2023 January, 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, 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 trainings, education 3
ICS conferences 5
ICS incidents 8
Book recommendation 9
ICS security news selection 10
ICS vulnerabilities 12
ICS alerts 18

ICS good practices, recommendations

5 Best Practices for Operational Technology (OT) Security

SCADAfence (Michael Yehoshua) published best practices to achieve Operational Technology security.

Modern operational technology (OT) networks are evolving due to developments such as the rise of Industrial Internet of Things (IIoT), Industry 4.0, smart grid and more. In order to remain competitive in their industries, organizations are adopting these beneficial technologies to optimize their operations and significantly cut operational costs.

These new technologies increase the connectivity and the complexity of operational environments, and as a result, their exposure to potential OT cyber attacks or damage caused by human error increases significantly. In the past, operators trusted network segmentation, isolation, or air-gapping as an effective security measure, but due to the increasing connectivity between the OT, IT and other networks, this is no longer true. Therefore, adhering to OT security best practices, and deploying the most advanced OT security tools is critical for the protection, visibility, and control of OT environments.

5 Best Practices For OT Security:

1. Automatic discovery, full visibility and management of OT asset inventory
2. Proactive, actionable warnings regarding risks and vulnerabilities in the OT network
3. Network mapping and connectivity analysis
4. Detection of suspicious activities, exposures, and malware attacks
5. Full, deep-packet analysis of the network & industrial equipment activities

Source and more information available on the following link:

https://blog.scadafence.com/5-ot-security-best-practices-for-industrial-digital-transformation

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in February 2023:

- 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&

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

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
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- 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/

- ICS/SCADA security training seminar

https://www.enoinstitute.com/scada-ics-security-training-seminar/

- 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 conferences

In February 2023, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Create The Future of OT and ICS Security at S4x23

Set free a conservative, slow moving, change resistant community to discover new ideas and come up with innovative ways to use these new ideas to deploy secure, resilient and better ICS.

After a Covid caused cancellation of S4x21 and delay until April of S4x22, a record 800 of the best talent in the ICS security community came together in Miami South Beach for S4x22.

Miami South Beach, USA; 13th – 16th February 2023

More details can be found on the following website:

https://s4xevents.com/

Airport Safety and Security Conference

The organizers are glad to invite you to our forthcoming "Airport Operations, Safety, and Security Conference," which will be held in Munich, Germany on February 16th and 17th, 2023. The Airport Operations, Safety, and Security conference bring together industry experts from airports, regulators, security agencies, and solution vendors. Along with examples of clear and current best practices for how our airports should tackle the latest security regulation and compliance demands.

The conference will also look at the latest security technologies used at airports and how security intelligence has fared against constantly changing security trends such as looking for drugs and related contraband, bomb and terror threats, and robberies, among other crimes perpetrated by criminals. Airports, by definition, provide significant planning, operational, and security issues, balancing the requirement to move people and cargo quickly and effectively while maintaining ever-increasing levels of security and safety.

Munich, Germany; 16th February 2023

More details can be found on the following website:

https://www.eventyco.com/event/airport-safety-and-security-conference-2022-munich-germany

ICIC 2023: 17. International Conference on Industrial Cybersecurity

International Conference on Industrial Cybersecurity aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Industrial Cybersecurity. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Industrial Cybersecurity.

Barcelona, Spain; 16th – 17th February 2023

More details can be found on the following website:

https://waset.org/industrial-cybersecurity-conference-in-february-2023-in-barcelona

14th SCADA World Summit

The 14th SCADA World Summit is dedicated to the implementation of highly effective and energy efficient SCADA system with a focus on growing business needs, security risks and challenges associated with SCADA implementation.

The 14th SCADA World Summit covers topics such as:

- System Implementation & Upgrade
- SCADA Data Analysis & Management
- Cyber Security Management
- IT/OT Integration
- SCADA System Design
- Minimizing System Downtime
- Internet of Things Applications for SCADA
- Transiting into Cloud SCADA Architecture

The 14th SCADA World Summit brings together senior attendees from power & utilities companies, global energy, gas & petrochemical companies, oil, manufacturing companies and transportation companies with responsibilities in:

- Industrial Control Systems
- SCADA
- Information Technology
- Information Systems
- Distribution
- Transmission
- System Planning

- Electrical/Systems Engineering
- Maintenance

Singapore, Singapore; 27th February – 2nd March 2023

More details can be found on the following website:

https://www.clocate.com/scada-world-summit/87555/

ICS incidents

Hacker selling data allegedly stolen from Volvo cars following ransomware attack

In the end of December 2022, Volvo suffered a Ransomware attack, named Endurance Ransomware. The attackers wanted to extort the Swedish vehicle manufacturer, but Volvo did not pay.

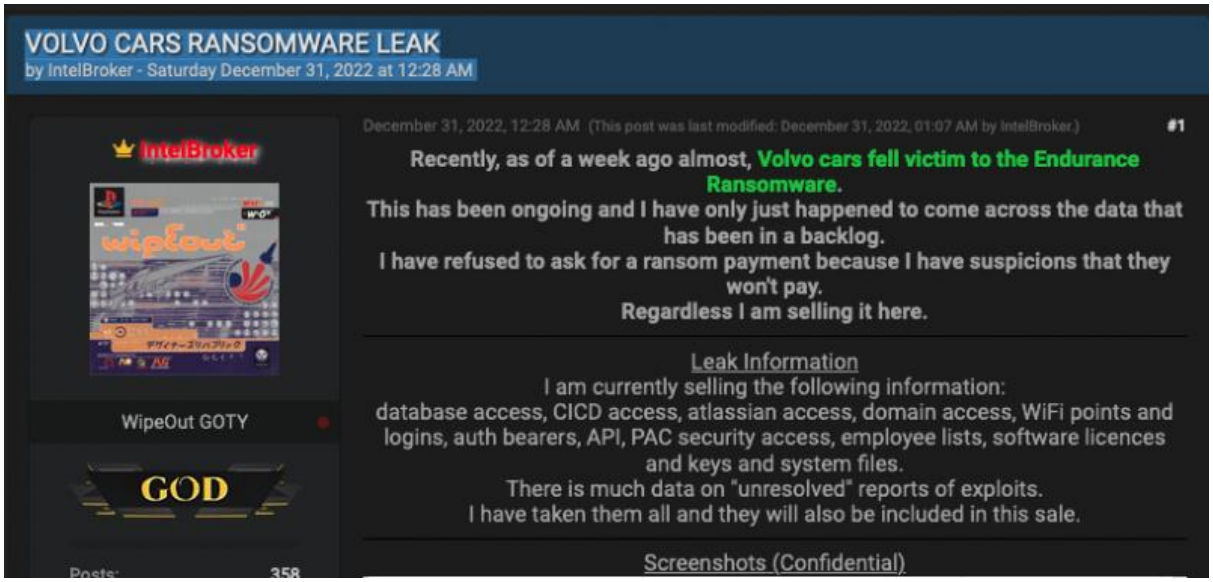
The attackers stole many sensitive information from the vehicle manufacturer, and they started to sell the stolen data. The Volvo data offered for sale — for the price of $2,500 in Monero cryptocurrency — allegedly includes information on existing and future vehicle models, databases, development systems, and employee information.

The company said that there was no impact on the safety or security of customer cars or their personal data.

There is no further information regarding the incident at this time.

The source and more information are available on the following links:

https://www.securityweek.com/hacker-selling-data-allegedly-stolen-volvo-cars-following-ransomware-attack



Source: https://www.securityweek.com/hacker-selling-data-allegedly-stolen-volvo-cars-following-ransomware-attack

Book recommendation

Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems

Although cybersecurity is something of a latecomer on the computer science and engineering scene, there are now inclinations to consider cybersecurity a meta-discipline. Unlike traditional information and communication systems, the priority goal of the cybersecurity of cyber-physical systems is the provision of stable and reliable operation for the critical infrastructures of all fundamental societal functions and activities. This book, Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems, presents the 28 papers delivered at the NATO Advanced Research Workshop (ARW) hosted in Baku, Azerbaijan, and held online from 27-29 October 2021. The inspiration and motivation behind the ARW stem from the growth in large-scale cyber attacks, the rising degree of complexity and sophistication of advanced threats, and the need to protect critical infrastructure by promoting and building a resilient system to promote the well-being of all citizens. The workshop covered a wide range of cybersecurity topics, permeating the main ideas, concepts and paradigms behind ICS and blended with applications and practical exercises, with overtones to IoT, IIoT, ICS, artificial intelligence, and machine learning. Areas discussed during the ARW included the cybersecurity of critical infrastructures; its educational and research aspects; vulnerability analysis; ICS/PLC/SCADA test beds and research; intrusion detection, mitigation and prevention; cryptography; digital forensics for ICS/PLCs; Industry 4.0 robustness and trustworthiness; and Cyber Fortress concept infused with practical training.

Investigating theoretical and practical problems involving the security of critical and essential infrastructure of each segment of contemporary societies, the book will be of interest to all those whose work involves cybersecurity.

Authors/Editors: Popov, O.B., Sukhostat, L.

Year of issue: 2022

The book is available at the following link:

https://www.iospress.com/catalog/books/cybersecurity-for-critical-infrastructure-protection-via-reflection-of-industrial

ICS security news selection

After targeting water sector, HC3 confirms Clop ransomware attacks against healthcare organizations

The U.S. Department of Health & Human Services' Health Sector Cybersecurity Coordination Center (HC3) confirmed that it is aware of attacks on the health and public health (HPH) sector by the Clop ransomware hacker group. The disclosure comes a few months after the Russian-based Cl0p ransomware hacker group breached water systems at the U.K. water supply company South Staffordshire.

"The Clop ransomware has been around since 2019, and even though the organization had several members arrested, its activity appeared to be uninterrupted," the HC3 wrote in its analyst note on Wednesday. "However, the gang has had difficulties getting victims to pay out on a ransom which has reportedly led to a change in their tactics that directly impacts the HPH sector." …

Source, and more information:

https://industrialcyber.co/medical/after-targeting-water-sector-hc3-confirms-clop-ransomware-attacks-against-healthcare-organizations/

The Impact of Geopolitics on CPS Security

The world changed fundamentally during the pandemic. Businesses were affected profoundly as they were forced to undergo digital transformation quickly to survive. And for organizations that were able to truly excel at it, digital transformation became a differentiating advantage. Of course, shareholders clearly saw the cost and competitive advantages of digital transformation and there is no turning back.

Our physical world has become very dependent on its digital components so we can share data and take advantage of simplified and more efficient workflows. The challenge now is that we are in a position of playing catch-up because all that extra connectivity needs to be secured. While the need to secure cyber-physical systems (CPS) is nothing new, the pandemic has escalated it in ways none of us could have anticipated or prepared for out of the gate. For example, who could have imagined a 63-fold increase in telehealth utilization or that 80% of remote-capable workers would continue to work remotely at least part of the time? …

Source, and more information:

https://www.securityweek.com/impact-geopolitics-cps-security

Compelling need to build ICS resiliency across OT and ICS environments in 2023

The growing prevalence of cybersecurity incidents targeting critical infrastructure environments, at times resulting in operational downtime, loss of production from destructive malware, or malicious insider activity, makes it imperative for these organizations to work on and structure their ICS resiliency framework. This year, as organizations continue to use OT (operational technology) infrastructure to monitor and control physical processes, operational environments remain at high cyber risk, as a result of global competition and geopolitical tensions. …

Source, and more information:

https://industrialcyber.co/features/compelling-need-to-build-ics-resiliency-across-ot-and-ics-environments-in-2023/

The NCSC for Startups programme is looking for innovative ideas to encrypt and secure the industrial internet of things

The UK's National Cyber Security Centre (NCSC), alongside innovation hub partner Plexal, are scouting emerging cyber talent to form the next cohort of startups to be inducted into the NCSC for Startups programme, this time with a focus on securing the industrial internet of things (IIoT) and developing resilient products. The next cycle of the NCSC for Startups programme, which has been running for six years and now comprises a community of more than 60 organisations, will begin in January 2023 and will equip founders with the specialised knowledge needed to develop, adapt and pilot their technologies and support the first steps in their businesses growth with support from various partners. …

Source, and more information:

https://www.computerweekly.com/news/252528053/Industrial-IoT-focus-of-next-NCSC-startup-challenge?&web_view=true

What to consider when budgeting for 2023's OT cybersecurity needs and wants

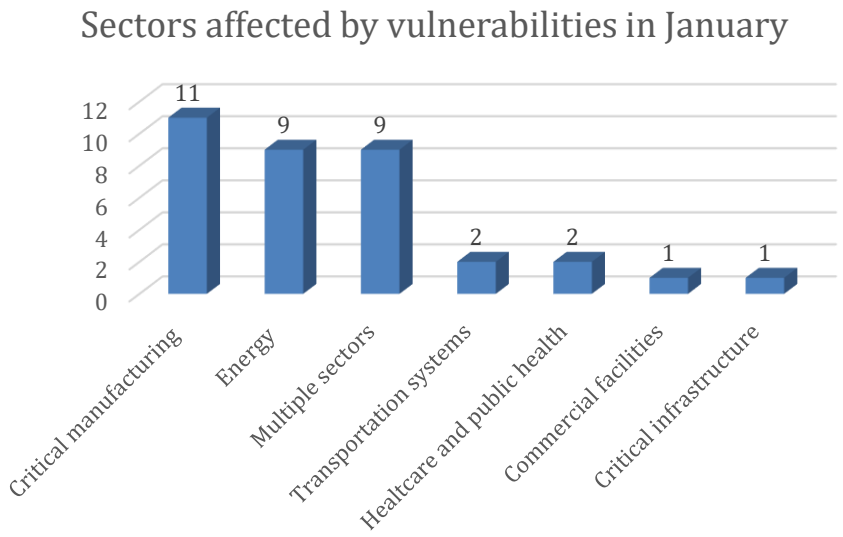
Regardless of what 2023 holds in store for the economy, your organization's financial commitment to supporting OT cybersecurity efforts is being decided now. In the public sector, much of the funding needed to secure critical infrastructure has already been allocated. But in the private sector funding is far from guaranteed. So how do you maximize your efforts, considering the current economic uncertainty and your need to protect assets? …

Source, and more information:

https://www.helpnetsecurity.com/2023/01/06/budgeting-ot-cybersecurity-2023/

ICS vulnerabilities

In January 2023, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

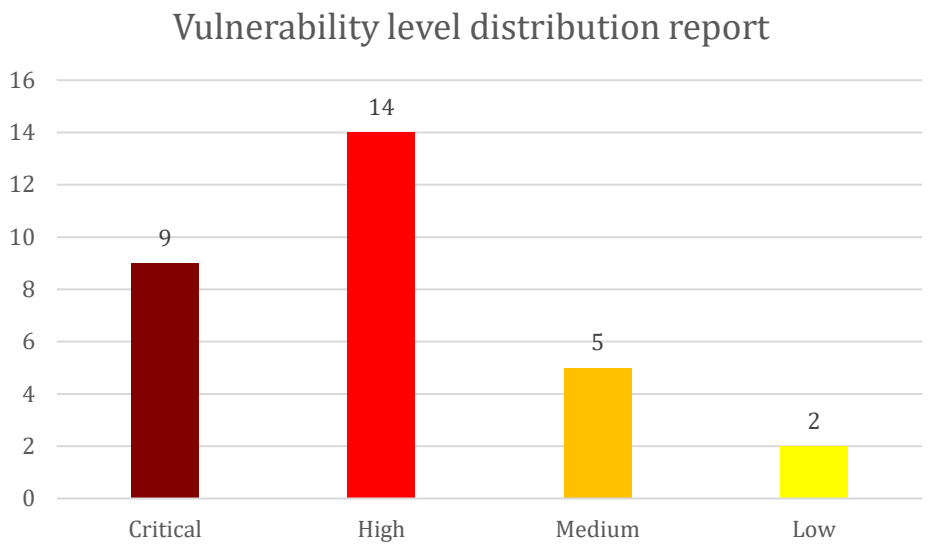


Average number of vulnerabilities per vulnerability report in January: **2,23**

Vulnerabilities/Exploitable remotely: **30/22**

The most common vulnerabilities in January:

Vulnerability	CWE number	Items
Path Traversal	CWE-22	4
Cleartext Transmission of Sensitive Information	CWE-319	4
Improper Access Control	CWE-284	4
OS Command Injection	CWE-78	3
Inadequate Encryption Strength	CWE-326	3
Use of Hard-coded Cryptographic Key	CWE-321	3



ICSA-23-026-01: **Delta Electronics CNCSoft ScreenEditor**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics CNCSoft ScreenEditor | CISA

ICSA-23-026-02: **Econolite EOS**

Critical level vulnerabilities: Improper Access Control, Use of Weak Hash.

Econolite EOS | CISA

ICSA-23-026-03: **Snap One Wattbox WB-300-IP-3**

High level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Heap-based Buffer Overflow, Plaintext Storage of a Password, Insufficient Verification of Data Authenticity.

Snap One Wattbox WB-300-IP-3 | CISA

ICSA-23-026-04: **Sierra Wireless AirLink Router with ALEOS Software**

High level vulnerabilities: Improper Neutralization of Argument Delimiters in a Command, Exposure of Sensitive Information to an Unauthorized Actor.

Sierra Wireless AirLink Router with ALEOS Software | CISA

ICSA-23-026-05: **Mitsubishi Electric MELFA SD/SQ series and F-series Robot Controllers**

High level vulnerability: Active Debug Code.

Mitsubishi Electric MELFA SD/SQ series and F-series Robot Controllers | CISA

ICSA-23-026-06: **Rockwell Automation products using GoAhead Web Server**

Critical level vulnerabilities: Infinite Loop, Use after Free.

Rockwell Automation products using GoAhead Web Server | CISA

ICSA-23-026-07: **Landis+Gyr E850**

Low level vulnerability: Reliance on Cookies without Validation and Integrity.

Landis+Gyr E850 | CISA

ICSA-23-017-02: **Mitsubishi Electric MELSEC iQ-F, iQ-R Series (Update A)**

Medium level vulnerability: Predictable Seed in Pseudo-Random Number Generator (PRNG).

Mitsubishi Electric MELSEC iQ-F, iQ-R Series (Update A) | CISA

ICSA-23-024-01: **XINJE XD**

High level vulnerabilities: Relative Path Traversal, Uncontrolled Search Path Element.

XINJE XD | CISA

ICSA-23-024-02: **SOCOMEC MODULYS GP**

Medium level vulnerability: Weak Encoding for Password.

SOCOMEC MODULYS GP | CISA

ICSA-23-019-01: **Hitachi Energy PCU400**

High level vulnerability: Reliance on Uncontrolled Component.

Hitachi Energy PCU400 | CISA

ICSA-23-017-01: **GE Digital Proficy Historian**

Critical level vulnerabilities: Authentication Bypass using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Weak Encoding for Password.

GE Digital Proficy Historian | CISA

ICSA-23-017-02: **Mitsubishi Electric MELSEC iQ-F, iQ-R Series**

Medium level vulnerability: Predictable Seed in Pseudo-Random Number Generator (PRNG).

Mitsubishi Electric MELSEC iQ-F, iQ-R Series | CISA

ICSA-23-017-03: **Siemens SINEC INS**

Critical level vulnerabilities: OS Command Injection, Inadequate Encryption Strength, Out-of-bounds Write, HTTP Request Smuggling, Inadequate Encryption Strength, Use of Insufficiently Random Values, Authentication Bypass by Spoofing, Path Traversal, Command Injection.

Siemens SINEC INS | CISA

ICSA-23-012-01: **Sewio RTLS Studio**

Critical level vulnerabilities: Use of Hard-coded Password, OS Command Injection, Out-of-bounds Write, Cross-Site Request Forgery, Improper Input Validation, Cross-site Scripting.

Sewio RTLS Studio | CISA

ICSA-23-012-02: **RONDS Equipment Predictive Maintenance Solution**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Path Traversal.

RONDS Equipment Predictive Maintenance Solution | CISA

ICSA-23-012-03: **InHand Networks InRouter**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, OS Command Injection, Use of a One-way Hash with a Predictable Salt, Improper Access Control, Use of Insufficiently Random Values.

InHand Networks InRouter | CISA

ICSA-23-012-04: **Panasonic Sanyo CCTV Network Camera**

High level vulnerability: Cross-Site Request Forgery (CSRF).

Panasonic Sanyo CCTV Network Camera | CISA

ICSA-23-012-05: **SAUTER Controls Nova 200 – 220 Series (PLC 6)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Cleartext Transmission of Sensitive Information.

SAUTER Controls Nova 200 – 220 Series (PLC 6) | CISA

ICSA-23-012-06: **Johnson Controls Metasys**

High level vulnerability: Insufficiently Protected Credentials.

Johnson Controls Metasys | CISA

ICSA-23-012-07: **Hitachi Energy Lumada APM**

Medium level vulnerability: Improper Access Control.

Hitachi Energy Lumada APM | CISA

ICSA-23-012-08: **Siemens S7-1500 CPU devices**

Low level vulnerability: Missing Immutable Root of Trust in Hardware.

Siemens S7-1500 CPU devices | CISA

ICSA-23-012-09: **Siemens Mendix SAML Module**

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

Siemens Mendix SAML Module | CISA

ICSA-23-012-10: **Siemens Automation License Manager**

High level vulnerabilities: External Control of File Name or Path, Path Traversal.

Siemens Automation License Manager | CISA

ICSA-23-012-11: **Siemens Solid Edge before V2023 MP1**

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

Siemens Solid Edge before V2023 MP1 | CISA

ICSMA-21-322-02: **Philips Patient Information Center iX (PIC iX) and Efficia CM Series (Update A)**

Medium level vulnerabilities: Improper Input Validation, Use of Hard-coded Cryptographic Key, Use of a Broken or Risky Cryptographic Algorithm.

Philips Patient Information Center iX (PIC iX) and Efficia CM Series (Update A) | CISA

ICSA-23-010-01: **Black Box KVM**

High level vulnerability: Path Traversal.

Black Box KVM | CISA

ICSA-23-005-01: **Hitachi Energy UNEM**

High level vulnerabilities: Inadequate Encryption Strength, Use of Hard-coded Cryptographic Key, Cleartext Transmission of Sensitive Information.

Hitachi Energy UNEM | CISA

ICSA-23-005-02: **Hitachi Energy FOXMAN-UN**

High level vulnerabilities: Inadequate Encryption Strength, Use of Default Cryptographic Key, Use of Hard-coded Cryptographic Key, Cleartext Transmission of Sensitive Information.

Hitachi Energy FOXMAN-UN | CISA

ICSA-23-005-03: **Hitachi Energy Lumada Asset Performance Management**

Critical level vulnerabilities: Classic Buffer Overflow, Out-of-bounds Write.

Hitachi Energy Lumada Asset Performance Management | CISA

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

https://ics-cert.us-cert.gov/advisories

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

In January 2023, ICS-CERT hasn't published alerts.