2021. December, 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 6

ICS INCIDENTS 7

BOOK RECOMMENDATION 8

BLACK CELL RECOMMENDATIONS 9

ICS VULNERABILITIES 10

ICS ALERTS 16

ICS good practices, recommendations

Good Practice Guide Process Control and SCADA Security

There are many SCADA security good practices on the web. Many of them are very useful. Centre for the Protection of National Infrastructure (UK) published a guide to improve the SCADA security.

The main contents of the guide are the followings:

- Securing process control and SCADA systems
- Understand the business risk
- Implement secure architecture
- Establish response capabilities
- Improve awareness and skills
- Manage third party risk
- Engage projects
- Establish ongoing governments

Good practice, in the context of the document, is defined as:

The best of industry practices such as strategies, activities, or approaches, which have been shown to be effective through research and evaluation. The good practices summarised in the document are intended only as guidelines. For some environments and process control systems, it may not be possible to implement all of these principles. For example:

- Good practice statement: Protect process control systems with anti-virus software on workstations and servers
- Complication: It is not always possible to implement anti-virus software on process control systems workstations or servers
- Good practice statement: Obtain vendor accreditation and configuration guidance from process control system vendors prior to deployment of such software
- Complication: Some vendors will not accredit anti-virus software and other process control systems are incompatible with such software.

Source and more information are available on the following link:

https://icscsi.org/library/Documents/Best_Practices/CPNI%20-%20GPG%20-%2000%20Process%20Control%20and%20SCADA%20Security.pdf

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in January 2022:

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours

- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - 17-22. January 2022
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 17-22. January 2022
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

The SCADAhacker.com website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

ICS conferences

In January 2022, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

CS4CA MENA summit

The MENA region is considered one of the world's most targeted regions for cyber-attacks, largely due to its rising populations, pre-existing political tensions and major industrial projects which are driving the next levels of innovation and digitalisation that aim to transform the future of the region. Although the region strives to be front-runners in digital innovation, the level of security maturity must be improved if they are to achieve this goal.

As OT environments continue to converge with IT networks the need to secure these technologies to support continuous uptime and safety, has never been more critical. In particular, for business leaders in the Oil & Gas, Chemical, Healthcare, Mining, Utility, Maritime, and other critical industries.

With this in mind, CS4CA MENA summit will explore all aspects of IT & OT security with a focus on digitally transforming critical infrastructures. The summit will bring together some of the brightest minds in the industry, uniting 100+ IT & OT security leaders online for 2 days of insight building, strategy planning and expert knowledge exchange on 24th – 25th January 2022.

Dubai, UAE; January 24-25, 2022

More details can be found on the following website:

https://mena.cs4ca.com/

S4X22

The conference's main issue is the OT and ICS security.

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. 719 of the world's best in OT and ICS Security attended S4x20. S4x21 was lost to Covid. Now S4x22 is coming back bigger and better.

S4x22 is 3 days on 3 stages plus an optional Monday training day. Of course, the content will be cutting edge and great. We know that interacting with your fellow attendees is key.

Miami, Florida, USA; 25-27. January 2022

More details can be found on the following website:

https://s4xevents.com/

ICS incidents

The 2021 State of Industrial Cybersecurity

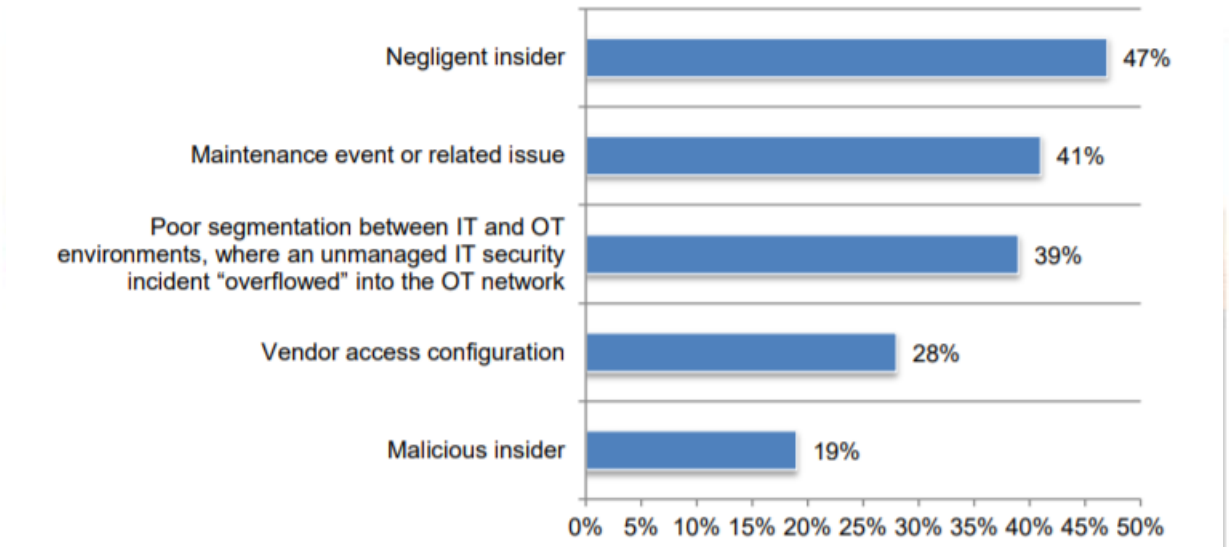
Ponemon Institute published a survey (sponsored by Dragos) from the Industrial Control System (ICS) and Operational Technology (OT) environments and the incidents, in November 2021.

The comprehensive IT/OT security establishment is very important. Many organizations (17%) are on the early stage of this work. The Mature stage is only 21%.

The primary challenge is to having OT and IT work cohesively are the cultural differences between engineers, security professionals, and IT staff (50%).

But our point of view in this section is the incidents.

The related organizations' cybersecurity incident causes are the followings:



The average time to detect the cybersecurity incident: 170 days. The average total hours to remediate one cybersecurity incident (316 days x 8 hours per workday): 2825 hours. The highest rate of the incident consequences: Loss of confidence in the system (54%).

Other interesting data and information is in the survey. Recommended to analyse the survey and draw the consequences.

The source and more information available at the following links:

https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en

Book recommendation

Secure Operations Technology

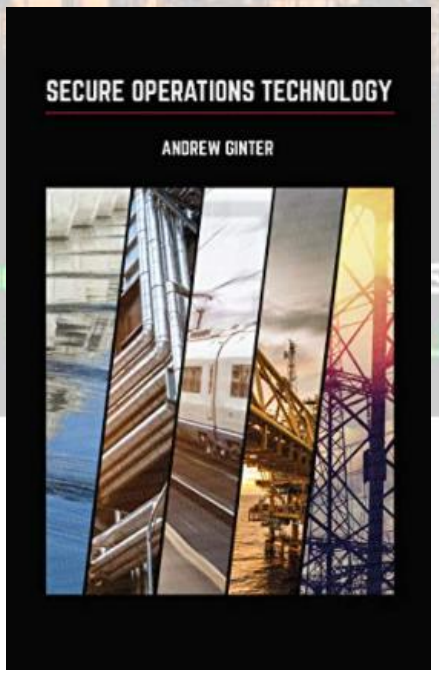
IT-SEC protects the information. SEC-OT protects physical, industrial operations from information, more specifically from attacks embedded in information. When the consequences of compromise are unacceptable – unscheduled downtime, impaired product quality and damaged equipment – software-based IT-SEC defences are not enough. Secure Operations Technology (SEC-OT) is a perspective, a methodology, and a set of best practices used at secure industrial sites. SEC-OT demands cyber-physical protections - because all software can be compromised. SEC-OT strictly controls the flow of information – because all information can encode attacks. SEC-OT uses a wide range of attack capabilities to determine the strength of security postures - because nothing is secure. This book documents the Secure Operations Technology approach, including physical offline and online protections against cyber-attacks and a set of twenty standard cyber-attack patterns to use in risk assessments.

Authors/Editors: Andrew Ginter

Year of issue: 2019

The book is available at the following link:

https://www.amazon.com/Secure-Operations-Technology-Andrew-Ginter-ebook/dp/B07NZ45Q93



Black Cell recommendations

Top 20 Secure PLC Coding Practices

Secure coding is a very important aspect to Programmable Logic Controllers security. PLC-security.com published a document, which can help to improve the secure PLC coding and contains 20 practices. The 20 practices are the following:

1. Modularize PLC Code
2. Track operating modes
3. Leave operational logic in the PLC wherever feasible
4. Use PLC flags as integrity checks
5. Use cryptographic and / or checksum integrity checks for PLC code
6. Validate timers and counters
7. Validate and alert for paired inputs / outputs
8. Validate HMI input variables at the PLC level, not only at HMI
9. Validate indirections
10. Assign designated register blocks by function (read/write/validate)
11. Instrument for plausibility checks
12. Validate inputs based on physical plausibility
13. Disable unneeded / unused communication ports and protocols
14. Restrict third-party data interfaces
15. Define a safe process state in case of a PLC restart
16. Summarize PLC cycle times and trend them on the HMI
17. Log PLC uptime and trend it on the HMI
18. Log PLC hard stops and trend them on the HMI
19. Monitor PLC memory usage and trend it on the HMI
20. Trap false negatives and false positives for critical alerts

Secure coding is one of the most important steps to establish an appropriate security. Recommended to follow these 20 points lists and the details.

If your PLC coding process is appropriate, this document can help to identify the gaps and you can improve your secure PLC coding system.

Source and more details available on the following link:

https://www.plc-security.com/

ICS vulnerabilities

In December 2021, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSA-21-357-01: **Moxa MGate Protocol Gateways**
Critical level vulnerability: Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-357-01

ICSA-21-357-02: **Johnson Controls exacq Enterprise Manager**
Critical level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-357-02

ICSMA-21-355-01: **Fresenius Kabi Agilia Connect Infusion System**
High level vulnerabilities: Uncontrolled Resource Consumption, Use of a Broken or Risky Cryptographic Algorithm, Insufficiently Protected Credentials, Improper Access Control, Plaintext Storage of a Password, Files or Directories Accessible to External Parties, Exposure of Information Through Directory Listing, Cross-site Scripting, Injection, Use of Hard-coded Credentials, Use of Client-side Authentication, Use of Unmaintained Third-party Components.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-355-01

ICSA-21-355-01: **mySCADA myPRO**
Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Use of Password Hash with Insufficient Computational Effort, Hidden Functionality, OS Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-355-01

ICSA-21-355-02: **Horner Automation Cscape EnvisionRV**
High level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-355-02

ICSA-21-355-03: **WECON LeviStudioU**
High level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-355-03

ICSA-21-355-04: **Emerson DeltaV**
High level vulnerabilities: Missing Authentication for Critical Function, Uncontrolled Search Path Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-355-04

ICSA-21-348-02: **Schneider Electric Rack PDU (Update A)**
Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-348-02

ICSA-21-350-01: **Xylem AquaView**
Critical level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-01

ICSA-21-350-02: Delta Electronics CNCSoft
Medium level vulnerability: Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-02

ICSA-21-350-03: Wibu-Systems CodeMeter Runtime
High level vulnerability: Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-03

ICSA-21-350-04: Mitsubishi Electric GX Works2
Medium level vulnerability: Improper Handling of Length Parameter Inconsistency.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-04

ICSA-21-350-05: Mitsubishi Electric FA Engineering Software
Medium level vulnerabilities: Out-of-bounds Read, Integer Underflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-05

ICSA-21-350-06: Siemens Capital VSTAR
High level vulnerabilities: Access of Resource Using Incompatible Type, Improper Validation of Specified Quantity in Input, Out-of-Bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Integer Underflow, Improper Handling of Inconsistent Structural Elements.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-06

ICSA-21-350-07: Siemens POWER METER SICAM Q100
Critical level vulnerability: Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-07

ICSA-21-350-08: Siemens JTTK and JT Utilities
High level vulnerabilities: Out-of-bounds Write, Use after Free, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-08

ICSA-21-350-09: Siemens SINUMERIK Edge
High level vulnerability: Improper Certificate Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-09

ICSA-21-350-10: Siemens JT2Go and Teamcenter Visualization
High level vulnerabilities: Out-of-Bounds Write, Use of Uninitialized Variable, Out-of-Bounds Read, Off-by-One Error, Use-after-Free.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-10

ICSA-21-350-11: Siemens SIMATIC eaSie PCS 7 Skill Package
Medium level vulnerability: Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-11

ICSA-21-350-12: Siemens SIMATIC ITC
Critical level vulnerability: Using Components with Known Vulnerabilities.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-12

ICSA-21-350-13: **Siemens Questa and ModelSim**
Critical level vulnerability: Insufficiently Protected Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-13

ICSA-21-350-14: **Siemens Siveillance Identity**
High level vulnerability: Exposure of Resource to Wrong Sphere.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-14

ICSA-21-350-15: **Siemens Simcenter STAR-CCM+ Viewer**
High level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-15

ICSA-21-350-16: **Siemens Healthineers syngo fastView**
High level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-16

ICSA-21-350-17: **Siemens JT Utilities and JT Open Toolkit**
High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Stack-based Buffer Overflow, Use After Free, Improper Restriction of Operations within the Bounds of a Memory Buffer, Heap-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-17

ICSA-21-350-18: **Siemens Teamcenter Active Workspace**
Medium level vulnerability: Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-18

ICSA-21-350-19: **Siemens SiPass Integrated**
High level vulnerability: Exposure of Resource to Wrong Sphere.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-19

ICSA-21-350-20: **Siemens JTTK and JT Utilities**
High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-20

ICSA-21-315-07: **Siemens Nucleus RTOS-based APOGEE and TALON Products** (Update A)
Critical level vulnerabilities: Type Confusion, Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-07

ICSA-21-238-03: **Delta Electronics DIAEnergie** (Update A)
Critical level vulnerabilities: Use of Password Hash with Insufficient Computational Effort, Authentication Bypass Using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, SQL Injection, Cross-site Request Forgery, Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-238-03

ICSA-21-217-01: HCC Embedded InterNiche TCP/IP stack, NicheLite (Update B)

Critical level vulnerabilities: Return of Pointer Value Outside of Expected Range, Improper Handling of Length Parameter Inconsistency, Use of Insufficiently Random Values, Improper Input Validation, Uncaught Exception, Numeric Range Comparison Without Minimum Check, Generation of Predictable Numbers or Identifiers, Improper Check or Handling of Exceptional Conditions, Improper Null Termination.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-217-01

ICSA-21-131-03: Siemens Linux-based Products (Update G)

High level vulnerability: Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-131-03

ICSA-20-324-05: Mitsubishi Electric MELSEC iQ-R Series (Update C)

High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-324-05

ICSA-20-105-06: Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update B)

High level vulnerability: Business Logic Errors.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-06

ICSA-20-014-05: Siemens TIA Portal (Update C)

High level vulnerability: Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-05

ICSA-21-348-01: Advantech R-SeeNet

High level vulnerabilities: SQL Injection, Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-348-01

ICSA-21-348-02: Schneider Electric Rack PDU

Medium level vulnerability: Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-348-02

ICSMA-21-152-01: Hillrom Medical Device Management (Update A)

Medium level vulnerabilities: Out-of-Bounds Write, Out-of-Bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-152-01

ICSMA-21-343-01: Hillrom Welch Allyn Cardio Products

High level vulnerability: Authentication Bypass Using an Alternate Path or Channel.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-343-01

ICSA-21-343-01: Hitachi Energy GMS600, PWC600, and Relion

High level vulnerability: Improper Access Controls.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-343-01

ICSA-21-343-02: WECON LeviStudioU

High level vulnerability: Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-343-02

ICSA-21-341-01: Hitachi Energy RTU500 OpenLDAP
High level vulnerabilities: Type Confusion, Reachable Assertion.
https://us-cert.cisa.gov/ics/advisories/icsa-21-341-01

ICSA-21-341-02: Hitachi Energy XMC20 and FOX61x
Critical level vulnerabilities: Weak Password Requirements, Missing Handler.
https://us-cert.cisa.gov/ics/advisories/icsa-21-341-02

ICSA-21-243-02: FANUC Robot Controllers
High level vulnerabilities: Integer Coercion Error, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-243-02

ICSA-21-336-01: Schneider Electric SESU
Low level vulnerability: Insufficient Entropy.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-01

ICSA-21-336-02: Johnson Controls Entrapass
High level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-02

ICSA-21-336-03: Distributed Data Systems WebHMI
Critical level vulnerabilities: Authentication Bypass by Primary Weakness, Unrestricted Upload of File with Dangerous Type.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-03

ICSA-21-336-04: Hitachi Energy RTU500 series BCI
High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-04

ICSA-21-336-05: Hitachi Energy Relion 670/650/SAM600-IO
High level vulnerability: Insecure Default Initialization of Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-05

ICSA-21-336-06: Hitachi Energy APM Edge
High level vulnerability: Using Components with Known Vulnerabilities.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-06

ICSA-21-336-07: Hitachi Energy PCM600 Update Manager
Medium level vulnerability: Improper Certificate Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-07

ICSA-21-336-08: Hitachi Energy RTU500 series
High level vulnerabilities: Observable Discrepancy, Buffer Over-read, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-336-08

ICSA-21-334-01: Xylem Aanderaa GeoView
High level vulnerability: SQL Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-334-01

ICSA-21-334-02: Mitsubishi Electric MELSEC and MELIPC Series
High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-334-02

ICSA-21-334-03: Delta Electronics CNCSoft
High level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-334-03

ICSA-21-334-04: Johnson Controls CEM Systems AC2000
High level vulnerability: Off-by-one Error.
https://us-cert.cisa.gov/ics/advisories/icsa-21-334-04

ICSA-21-334-05: Hitachi Energy Retail Operations and CSB Software
High level vulnerability: Improper Access Control.
https://us-cert.cisa.gov/ics/advisories/icsa-21-334-05

ICSA-21-280-05: InHand Networks IR615 Router (Update A)
Critical level vulnerabilities: Improper Restriction of Rendered UI Layers or Frames, Improper Authorization, Cross-site Request Forgery, Inadequate Encryption Strength, Improper Restriction of Excessive Authentication Attempts, Unrestricted Upload of File with Dangerous Type, Cross-site Scripting, OS Command Injection, Observable Response Discrepancy, Weak Password Requirements.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-05

ICSA-21-119-04: Multiple RTOS (Update D)
Critical level vulnerability: Integer Overflow or Wraparound.
https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04

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 December 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

https://www.us-cert.gov/ics/alerts