2021. November, 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

Top 5 ICS Security Best Practices

There are many best practices in the field of ICS/SCADA security. Many of these are usually mentioning the same things, which are important for the industrial cybersecurity.

Each best practice collection contains an individual “thinking”, what if you think further, you get a new perspective to increase your ICS/SCADA security.

The study on the below link states, that cyber-physical systems are exposed to cyberattacks, and the number of insider threats are growing increasingly.

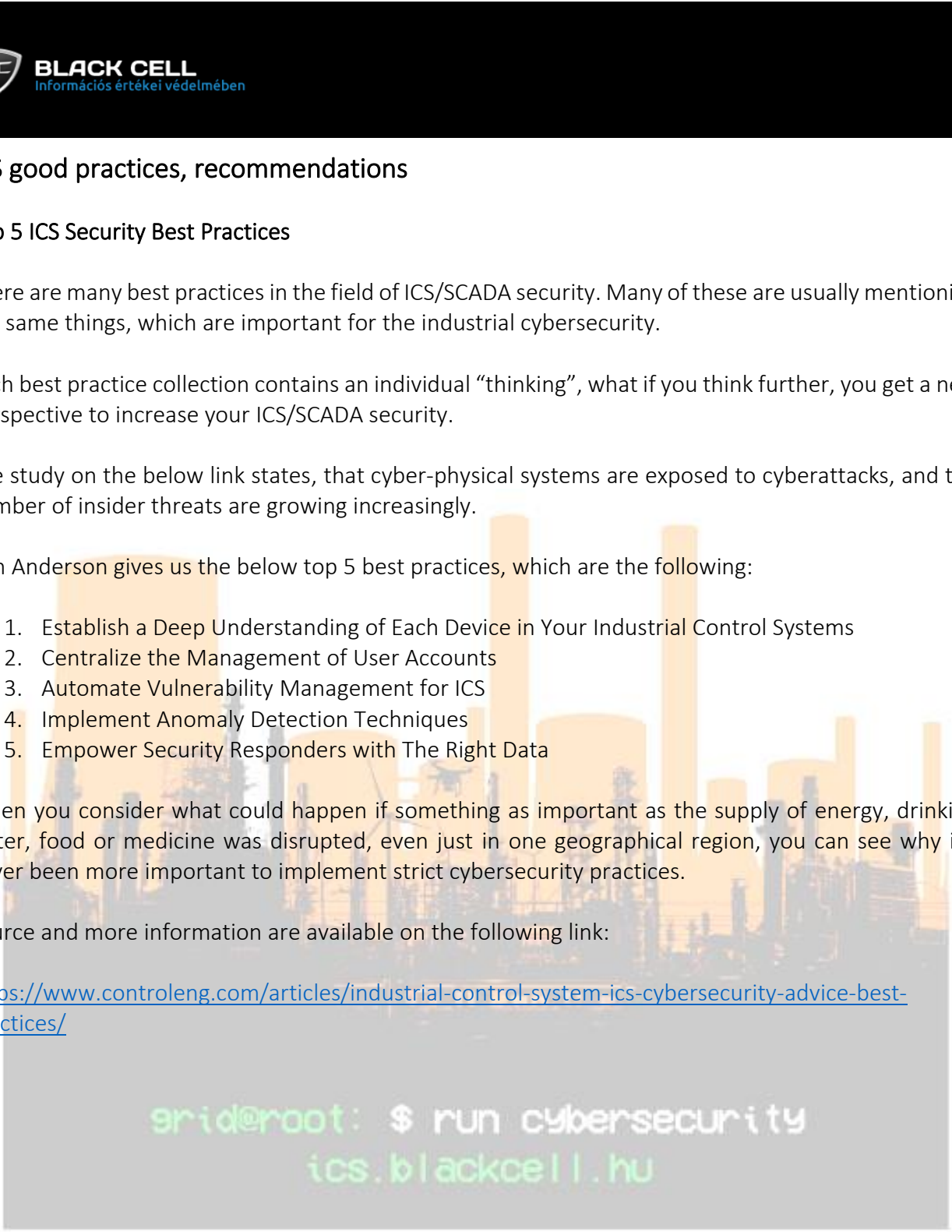
Erin Anderson gives us the below top 5 best practices, which are the following:

1. Establish a Deep Understanding of Each Device in Your Industrial Control Systems
2. Centralize the Management of User Accounts
3. Automate Vulnerability Management for ICS
4. Implement Anomaly Detection Techniques
5. Empower Security Responders with The Right Data

When you consider what could happen if something as important as the supply of energy, drinking water, food or medicine was disrupted, even just in one geographical region, you can see why it’s never been more important to implement strict cybersecurity practices.

Source and more information are available on the following link:

https://www.controleng.com/articles/industrial-control-system-ics-cybersecurity-advice-best-practices/



ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in December 2021:

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
  - 13-18. December 2021
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 13-18. December 2021
  - 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/

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 December 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

The World Congress on Industrial Control Systems Security (WCICSS-2021)

The conference is a meeting point for professionals and researchers, IT security professionals, managers, developers, educators, vendors and service providers who are involved in development, integration, assessment, implementation, and operation of industrial cybersecurity technologies. The WCICSS is an international refereed conference dedicated to the advancement of the theory and practices of Industrial Controls Security and SCADA. Therefore, the conference will provide opportunities to discuss both the current status and emerging trends in protection of industrial control systems.

The objectives of the WCICSS are to bridge the knowledge gap between academia and industry, promote research esteem in Industrial Control Systems Security and the importance of Intelligent Control Applications.

London, United Kingdom (virtual conference); 07-09. December 2021

More details can be found on the following website:

https://wcicss.org/

15. International Conference on Industrial Cybersecurity

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics, and industry researchers.

Rome, Italy; December 13-14, 2021

More details can be found on the following website:

https://waset.org/industrial-cybersecurity-conference-in-december-2021-in-rome

ICS incidents

Fuel Supply incident due to a cyberattack in Iran

Some fuel stations closed in Iran for a relatively long time, and the Supreme National Security Council confirmed, that the reason is a cyberattack. Further details are not known.

Many of the Iranians couldn't get petrol because of the IT system was blocked that allows Iranians to fill their tanks for free or at subsidised prices with a digital card issued by authorities.

The oil ministry said only the sales with smart cards used for cheaper rationed gasoline were disrupted and clients could still buy fuel at higher rates, as the ministry's news agency SHANA reported.

Someone also hacked the digital street signs, where people could read that "Khamenei, where is our gasoline?". "Plan B" came into force in this situation in many petrol stations, where the technicians rushed to activate manual settings after online functions were paralysed by hackers.

The semi-official ISNA news website published a story saying the petrol distribution system and the digital city monitors were hacked, but later it said its website was targeted by a cyberattack and the hackers published this story.

The sources and more information available at the following links:

https://www.securityweek.com/iran-blames-cyberattack-fuel-supply-hit

https://www.reuters.com/world/middle-east/iran-says-cyberattack-behind-widespread-disruption-gas-stations-2021-10-26/

https://www.aljazeera.com/news/2021/10/26/cyberattack-affects-petrol-stations-across-iran

https://www.dw.com/en/iran-cyberattack-targets-gas-stations-and-alters-billboards/a-59629503

Book recommendation

Cyber Security of Industrial Control Systems in the Future Internet Environment

In today's modernized market, internet-based technologies are widespread in the everyday operation of every aspect of society and businesses. The industrial sector is no different as these technological solutions have provided several benefits including reduction of costs, increasing scalability, and efficiency improvements. Despite this, Cyber Security remains a crucial risk factor in Industrial Control Systems. However, the same public and corporate solutions do not apply to this specific segment, because these security issues are more complex and intensive. Research is needed that explores new risk assessment methods and security mechanisms that professionals can apply to their modern technological procedures.

Cyber Security of Industrial Control Systems in the Future Internet Environment is a pivotal reference source that provides vital research on current security risks in critical infrastructure schemes with the implementation of information and communication technologies. While highlighting topics such as intrusion detection systems, forensic challenges, and smart grids, this publication explores specific security solutions within industrial sectors that have begun applying internet technologies to their current methods of operation. This book is ideally designed for researchers, system engineers, managers, networkers, IT professionals, analysts, academicians, and students seeking a better understanding of the key issues within securing industrial control systems that utilize internet technologies.

Authors/Editors: Mirjana D. Stojanovi (Author, Editor), Slavica V. Botjani Rakas (Editor)

Year of issue: 2020

The book is available at the following link:

https://www.amazon.com/Security-Industrial-Internet-Environment-Information/dp/1799829103

Black Cell recommendations

Threat landscape

CISA published the Threat landscape 2021 document, which shows the threats that might affect critical infrastructure and the industrial sector.

Increase in targeted ICS networks

The digital transformation makes the ICS networks exposed to the cyber attacks due to the increased number of IoT and the cloud usage. In the last years, four groups were discovered, who targeted the ICS networks. These groups are the following: STIBNITE, TALONITE, KAMACITE, and VANADINITE.

Cybercrime attacks increasingly target and impact critical infrastructure. During the reporting period, we observed increased targeting of critical infrastructure by cybercrime actors. Major critical infrastructure sectors being impacted are the healthcare, transportation, and energy sectors.

Disruption of illegal cryptomining operations are threats and the ICS operators also must handle this kind of threats like many of the examples in the 5.1.6. point of the document.

Ransomware is always hot topic and publications focused of these threats. The ransomware attack against Colonial Pipeline (a US fuel company) by the Darkside ransomware group had a high impact as a perceived gas shortage led to stockpiling and panic (although the IT network was impacted, operators stopped ICS operations for protection). Regarding the targeting of ICS networks, there has been an increase in public and non-public ransomware events affecting ICS environments.

The publication mentioned that CISA is published a tool, which can help to evaluate the level of readiness against ransomware of the ICS operators. It's recommended to use it, as if the organization knows the level of readiness and maturity, the improvement of the security posture will be easier.

There are some details in the document about the types of ransomware, for example Revil, which are very useful to identify if the organization has been involved.

It's recommended to read the publication, analyse the trends and implement the recommendations.

Source and more details available on the following link:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ICS vulnerabilities

In November 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:

ICSMA-21-322-01: **Philips IntelliBridge EC 40 and EC 80 Hub**

High level vulnerabilities: Use of Hard-coded Credentials, Authentication Bypass Using an Alternate Path or Channel.
https://us-cert.cisa.gov/ics/advisories/icsma-21-322-01

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

Medium level vulnerabilities: Improper Input Validation, Use of Hard-coded Cryptographic Key, Use of a Broken or Risky Cryptographic Algorithm.
https://us-cert.cisa.gov/ics/advisories/icsma-21-322-02

ICSA-21-266-01: **Trane Symbio (Update A)**

High level vulnerability: Code Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-266-01

ICSMA-20-254-01: **Philips Patient Monitoring Devices (Update B)**

Medium level vulnerabilities: Improper Neutralization of Formula Elements in a CSV File, Cross-site Scripting, Improper Authentication, Improper Check for Certificate Revocation, Improper Handling of Length Parameter Inconsistency, Improper Validation of Syntactic Correctness of Input, Improper Input Validation, Exposure of Resource to Wrong Sphere.
https://us-cert.cisa.gov/ics/advisories/icsma-20-254-01

ICSA-20-212-04: **Mitsubishi Electric Factory Automation Engineering Products (Update E)**

High level vulnerability: Unquoted Search Path or Element.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04

ICSA-20-084-01: **VISAM Automation Base (VBASE) (Update B)**

Critical level vulnerabilities: Relative Path Traversal, Incorrect Default Permissions, Inadequate Encryption Strength, Insecure Storage of Sensitive Information, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-084-01

ICSA-21-320-01: **FATEK Automation WinProladder**

High level vulnerabilities: Out-of-bounds Write, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-320-01

ICSA-21-320-02: **Mitsubishi Electric GOT products**

High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-320-02

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

High level vulnerabilities: Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency.
https://us-cert.cisa.gov/ics/advisories/icsa-21-049-02

ICSA-21-315-01: **WECON PLC Editor**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-01

ICSA-21-315-02: **Multiple Data Distribution Service (DDS) Implementations**

High level vulnerabilities: Write-what-where Condition, Improper Handling of Syntactically Invalid Structure, Network Amplification, Incorrect Calculation of Buffer Size, Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency, Amplification, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-02

ICSA-21-315-03: **Siemens SIMATIC WinCC**

Critical level vulnerabilities: Path Traversal, Insertion of Sensitive Information into Log File.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-03

ICSA-21-315-04: **Siemens Mendix**

Low level vulnerability: Use of Web Browser Cache Containing Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-04

ICSA-21-315-05: **Siemens Mendix Studio Pro**

Medium level vulnerability: Incorrect Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-05

ICSA-21-315-06: **Siemens SCALANCE W1750D**

Critical level vulnerabilities: Improper Restriction of Operations Within the Bounds of a Memory Buffer, Command Injection, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-06

ICSA-21-315-07: **Siemens Nucleus RTOS-based APOGEE and TALON Products**

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://us-cert.cisa.gov/ics/advisories/icsa-21-315-07

ICSA-21-315-08: **Siemens NX OBJ Translator**

High level vulnerabilities: Use After Free, Access of Uninitialized Pointer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-08

ICSA-21-315-09: **Siemens Climatix POL909**

Medium level vulnerability: Missing Encryption of Sensitive Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-09

ICSA-21-315-10: **Siemens SENTRON powermanager**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-10

ICSA-21-315-11: Siemens SIMATIC RTLS Locating Manager

Medium level vulnerabilities: Insertion of Sensitive Information into Log File, Cleartext Storage of Sensitive Information, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-11

ICSA-21-315-12: Siemens NX JT Translator

Low level vulnerabilities: Out-of-bounds Read, Access of Uninitialized Pointer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-12

ICSA-21-315-13: Siemens Siveillance Video DLNA Server

High level vulnerability: Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-315-13

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

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

ICSA-21-103-04: Siemens Nucleus Products DNS Module (Update A)

High level vulnerabilities: Out-of-bounds Write, Use of Out-of-Range Pointer Offset.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-04

ICSA-21-103-05: Siemens Nucleus Products IPv6 Stack (Update A)

High level vulnerability: Infinite Loop.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05

ICSA-21-042-01: Multiple Embedded TCP/IP Stacks (Update B)

High level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-042-01

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update H)

Medium level vulnerability: Unquoted Search Path or Element.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSMA-21-313-01: Philips MRI 1.5T and 3T

Medium level vulnerabilities: Improper Access Control, Incorrect Ownership Assignment, Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsma-21-313-01

ICSA-21-313-01: Schneider Electric NMC cards and Embedded Devices

Medium level vulnerabilities: Cross-site Scripting, Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-313-01

ICSA-21-313-02: Schneider Electric GUIcon

High level vulnerabilities: Out-of-bounds Write, Use After Free, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-313-02

ICSA-21-313-03: Siemens Nucleus RTOS TCP/IP Stack

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://us-cert.cisa.gov/ics/advisories/icsa-21-313-03

ICSA-21-313-04: mySCADA myDESIGNER

High level vulnerability: Relative Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-313-04

ICSA-21-313-05: OSIsoft PI Vision

Medium level vulnerabilities: Cross-site Scripting, Incorrect Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-313-05

ICSA-21-313-06: OSIsoft PI Web API

Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-313-06

ICSA-21-173-01: Advantech WebAccess HMI Designer (Update A)

High level vulnerabilities: Heap-based Buffer Overflow, Out-of-bounds Write, Improper Restriction of Operation Within the Bounds of a Memory Buffer, Use After Free, Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-173-01

ICSMA-21-308-01: Philips Tasy EMR

High level vulnerability: SQL Injection.
https://us-cert.cisa.gov/ics/advisories/icsma-21-308-01

ICSA-21-308-01: VISAM VBASE Editor

High level vulnerabilities: Improper Access Control, Cross-site Scripting, Improper Restriction of XML External Entity Reference, Using Components with Known Vulnerabilities.
https://us-cert.cisa.gov/ics/advisories/icsa-21-308-01

ICSA-21-308-02: AzeoTech DAQFactory

High level vulnerabilities: Use of Inherently Dangerous Function, Deserialization of Untrusted Data, Cleartext Transmission of Sensitive Information, Modification of Assumed-Immutable Data (MAID).
https://us-cert.cisa.gov/ics/advisories/icsa-21-308-02

ICSA-21-306-01: Sensormatic Electronics VideoEdge

Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-306-01

ICSA-18-277-01: WECON PI Studio (Update A)

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write, Information Exposure Through XML External Entity Reference, Out-of-bounds Read.

https://us-cert.cisa.gov/ics/advisories/ICSA-18-277-01

ICSA-21-301-01: Sensormatic Electronics victor
High level vulnerability: Use of Hard-coded Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-301-01

ICSA-21-280-04: Mitsubishi Electric MELSEC iQ-R Series C Controller Module (Update A)
Medium level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-04

ICSA-21-238-04: Delta Electronics DOPSoft (Update A)
High level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-238-04

ICSA-21-299-01: Fuji Electric Tellus Lite V-Simulator and V-Server Lite
High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write, Untrusted Pointer Dereference, Out-of-bounds Read, Access of Uninitialized Pointer, Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-299-01

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 November 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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