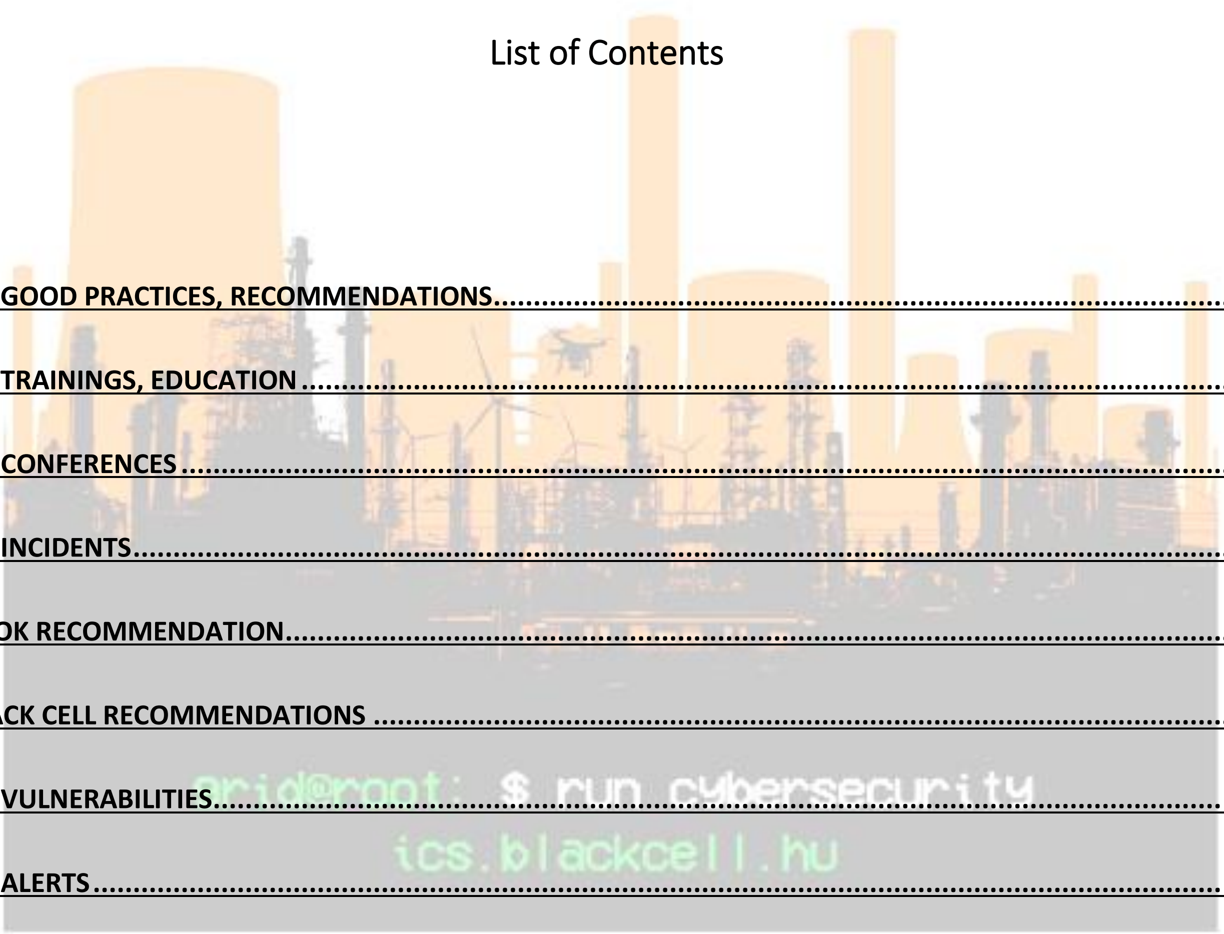
2021. January, Industrial Control Systems security feed

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, furthermore 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 cara@blackcell.hu.

List of Contents



ICS good practices, recommendations

Cyber Security Handbook for Electrical Industrial Control Systems

SeConSys is a non-profit, voluntary cooperation of leading Hungarian electricity protection, control technology, cyber security, electricity generation and service companies, regulatory and supervisory organizations, as well as energy and cyber security professionals.

In 2020 SeConSys editioned a handbook which made for the ICS/SCADA operators. The handbook has been prepared by processing a number of international regulations in the electricity sector (for example: German, Swiss, USA), taking into account domestic legal and other regulations, standards and recommendations, which may help the operators of designated critical infrastructures to enhance cyber security.

The handbook contains a threat map of ICS/SCADA systems, which can be used to identify industry risks that may be relevant in today's growing number of cyberattacks, making it easier for readers to identify cyber risks.

The handbook introduced many analyses in the field of ICS/SCADA security to help understanding the challenges. Reading this handbook is recommended for all experts and managers who are developers, manufacturers, operators, users and safety professionals of ICS/SCADA systems in the Electrical Network Operator sector.

The handbook available at the following link:

https://www.seconsys.eu/

SeConSys
Security for Control Systems

Villamosenergetikai ipari felügyeleti
rendszerek kiberbiztonsági kézikönyve

NEMZETI
KIBERVÉDELMI INTÉZET

ICS trainings, education

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

SANS provides online ICS security courses due to the COVID-19 pandemic situation.

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 security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

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 (210W-10) – 1.5 hours

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
  - 01-06. February 2021.

- ICS515: ICS Active Defense and Incident Response
  - only from March

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

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:

- Understanding, Assessing and Securing Industrial Control Systems

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

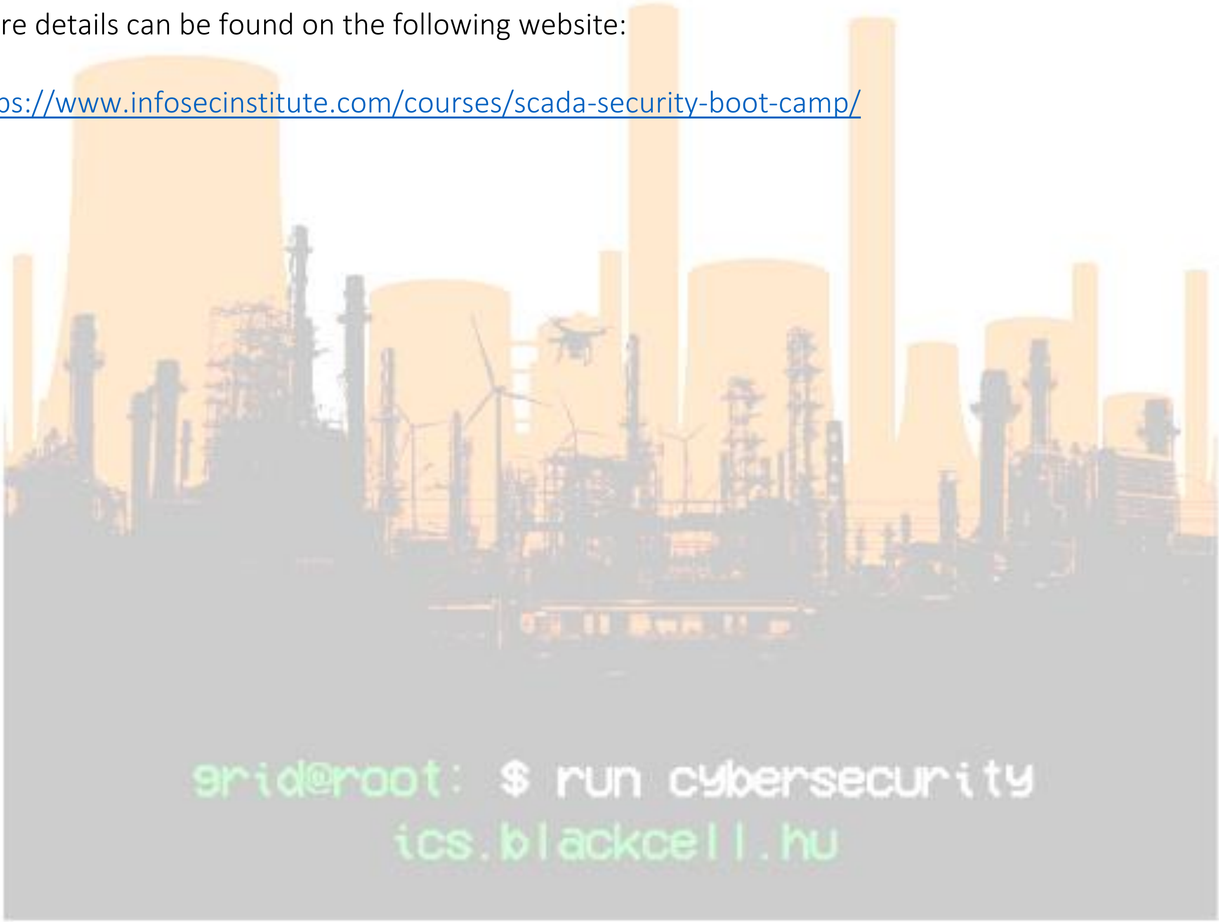
INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the “Certified SCADA Security Architect” certification for the candidates.

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/



ICS conferences

In February 2021, in light of the COVID-19 pandemic, many ICS/SCADA security conferences and workshops are held in virtual (not comprehensive):

M01 Industrial Control Systems Security

Participants will learn about the safety and security fundamentals of industrial control systems. Incidents affecting ICS systems, terminology, and case studies will be presented in the conference.

The ICS threat modelling is also part of the conference, and the participants can learn about the relevant risk assessment methodologies, detecting cyberattacks, and the speakers introduces good practices and the future challenges of the ICS Security.

(Online); 01-05. February 2021.

More details can be found on the following website:

https://www.date-conference.com/tutorial/m01

Cyber Security for Critical Assets Conference

The conference introduces the MENA critical infrastructures protection systems. IT and OT security professionals also participating in the conference as speakers, and they presented on how to grow the cyber resilience of an ICS system.

How to build a human firewall promises to be an interesting topic. The role of artificial intelligence in critical infrastructure protection is also presented.

(Online); 01-02. February 2021.

More details can be found on the following website:

https://mena.cs4ca.com/overview/

ICS incidents

Power outage in India that could have been caused by hackers

In October 2020, there was a major power outage in Mumbai, India’s largest city, which caused by a cyberattack according to the news of SecurityWeek. Restoration of vital services took 2 hours and took 12 hours while power supply was restored.

According to the cyber security police, it was not a sabotage, but a cyberattack that caused the power outage. Mumbai Mirror said investigators found several suspicious logins on the servers that were connected to the power supply and transmission utilities. It is hypothesized that manipulation of these servers may have caused the outage.

In tracing the activity, South Asian countries are suspected behind the attacks. According to the sources, the purpose of the attack was to make profit. Since February 2020, a number of cyberattacks have been launched against Indian power companies, including ransomware, BGP hijacking, and Distributed Denial of Service (DDoS).

India Today reported that malware was discovered by investigators at a power distribution center where the outage allegedly occurred. These centers are responsible for ensuring and monitoring the operation of the electrical grid and for scheduling and transmitting electricity generation.

There are a number of hacker groups that are known to attack organizations in the electricity sector, including a group linked to North Korea.

As a result of the power outage, public transport also stopped in Mumbay, making the lives of millions of people more complicated. There are also a number of videos on the Internet that can be used to monitor the effects of a power outage.

More details can be found on the following website:

https://www.securityweek.com/major-power-outage-india-possibly-caused-hackers-reports

Author: We don’t have enough information about this incident as unfortunately details were not disclosed about it. This non-disclosure is problematic, as information about the attack could be used to harden defenses for organizations engaged in similar activities. However, it can be stated that the ransomware attack is usually present in the repertoire of all cyber armies, so it is worthwhile to give priority to protection against ransomware among the prevention activities.

Book recommendation

Programmable Logic Controllers

In the latest 6th edition of the book, the author explains the basics of programmable logic units (PLCs), regardless of manufacturer. The book helps to understand the design, characteristics, internal architecture of PLCs, the principles of operation and last but not least the safety problems, fault detection and testing methodologies.

The new Chapter 1 of the latest release deals with the comparison of relay-controlled systems, microprocessor-controlled systems, and programmable logic controllers, along with an overview of PLC hardware and architecture. The book also includes examples from various PLC manufacturers, IEC programming standard references, function diagrams, and a number of case studies.

This book is recommended for those who want a deeper understanding of the mysteries of PLC operation.

Authors/Editors: William Bolton

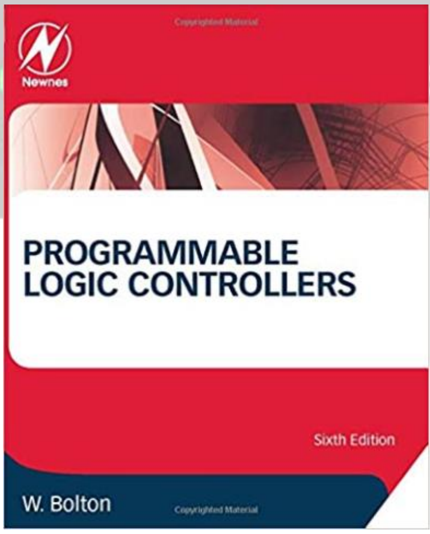
Year of issue: 2015.

The book available at the following link:

https://www.amazon.com/Programmable-Logic-Controllers-William-Bolton/dp/0128029293

The 4th edition of the publication is available in PDF at the following link:

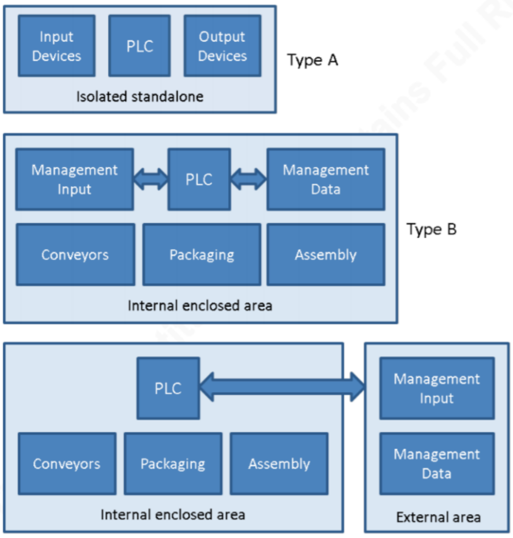
https://www.etf.ues.rs.ba/~slubura/Procesni%20racunari/Programmable%20Logic%20Controllers%204th%20Edition%20(W%20Bolton).pdf



Black Cell recommendations

Security needs of Programmable Logic Controllers

SANS information security documents include a Whitepaper that addresses security issues with programmable logic controllers (PLCs). There are 3 types of models, which are:



Type "A" is the isolated standalone model, model "B" is the internal closed area model, and type "C" is connected to the internal closed area model by an external area management system.

The whitepaper demonstrates what kinds of threats are affecting the different types of models and what vulnerabilities to face in their case.

The integrity of PLC devices is also addressed in the document, as well as the authentication and access issues, communication protection, and network and system protection. Information is also available to the reader of the document on how to increase the level of security.

In conclusion, the author notes that although a PLC is only a component of ICS systems and depends on many technical elements, it forms a system with several components. These elements are technological and non-technological components (such as administrative physical and logical protection measures) that together enhance the level of security.

We recommend reading the whitepaper for more details.

Whitepaper is available at the following link:

https://www.sans.org/reading-room/whitepapers/threats/plc-device-security-tailoring-37612

ICS vulnerabilities

In January 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-21-028-01: **Rockwell Automation FactoryTalk Linx and FactoryTalk Services Platform**
High level vulnerabilities: Classic Buffer overflow, Improper Check or Handling of Exceptional Conditions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-028-01

ICSA-21-026-01: **Fuji Electric Tellus Lite V-Simulator and V-Server Lite**
High level vulnerabilities: Stack-based Buffer Overflow, Out-of-Bounds Read, Out-of-Bounds Write, Access of Uninitialized Pointer, Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-026-01

ICSA-21-007-03: **Eaton EASYsoft** (Update A)
Medium level vulnerabilities: Type Confusion, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-03

ICSA-20-353-01: **Treck TCP/IP Stack** (Update A)
Critical level vulnerabilities: Heap-based Buffer Overflow, Out-of-bounds Read, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-20-353-01

ICSA-20-245-01: **Mitsubishi Electric Multiple Products** (Update A)
High level vulnerabilities: Predictable Exact Value from Previous Values.
https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01

ICSA-21-021-01: **Delta Electronics ISPSoft**
High level vulnerability: Use After Free.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-01

ICSA-21-021-02: **Delta Electronics TPEditor**
High level vulnerability: Untrusted Pointer Dereference, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-02

ICSA-21-021-03: **Honeywell OPC UA Tunneller**
Critical level vulnerabilities: Heap-based Buffer Overflow, Out-of-bounds Read, Improper Check for Unusual or Exceptional Conditions, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-03

ICSA-21-021-04: **Mitsubishi Electric MELFA**
High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-04

ICSA-21-021-05: **WAGO M&M Software fdtCONTAINER**
High level vulnerability: Deserialization of Untrusted Data.

https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05

ICSMA-21-019-01: **Philips Interventional Workstations**

Medium level vulnerability: OS Command Injection.
https://us-cert.cisa.gov/ics/advisories/icsma-21-019-01

ICSA-21-019-01: **Dnsmasq by Simon Kelley**

High level vulnerabilities: Heap-based Buffer Overflow, Insufficient Verification of Data Authenticity, Use of a Broken or Risky Cryptographic Algorithm.
https://us-cert.cisa.gov/ics/advisories/icsa-21-019-01

ICSA-21-019-02: **Reolink P2P Cameras**

Critical level vulnerabilities: Use of Hard-coded Cryptographic Key, Cleartext Transmission of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsa-21-019-02

ICSA-20-212-03: **Mitsubishi Electric Factory Automation Products Path Traversal (Update A)**

High level vulnerability: Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03

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

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

ICSMA-21-012-01: **SOOIL Dana Diabecare RS Products**

High level vulnerabilities: Use of Hard Coded Credentials, Insufficiently Protected Credentials, Use of Insufficiently Random Values, Use of Client-side Authentication, Client-side Enforcement of Server-side Security, Authentication Bypass by Capture-Replay, Unprotected Transport of Credentials, Key Exchange Without Entity Authentication, Authentication Bypass by Spoofing.
https://us-cert.cisa.gov/ics/advisories/icsma-21-012-01

ICSA-21-012-01: **Schneider Electric EcoStruxure Power Build-Rapsody**

High level vulnerability: Unrestricted Upload of File with Dangerous Type.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-01

ICSA-21-012-02: **Siemens SCALANCE X Switches**

Critical level vulnerability: Use of Hard-coded Cryptographic Key.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-02

ICSA-21-012-03: **Siemens JT2Go and Teamcenter Visualization**

High level vulnerabilities: Type Confusion, Improper Restriction of XML External Entity Reference, Out-of-bounds Write, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Untrusted Pointer Dereference, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-03

ICSA-21-012-04: **Siemens Solid Edge**

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

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-04

ICSA-21-012-05: Siemens SCALANCE X Products

Critical level vulnerabilities: Missing Authentication for Critical Function, Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05

ICSA-20-196-07: Siemens Opcenter Execution Core (Update B)

High level vulnerabilities: Cross-site Scripting, SQL Injection, Improper Access Control, Insufficiently Protected Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-07

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

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

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

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

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update C)

High level vulnerability: Resource Exhaustion.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update F)

High level vulnerability: Incorrect Calculation of Buffer Size.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-06

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

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

ICSA-19-283-02: Siemens PROFINET Devices (Update I)

High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02

ICSMA-21-007-01: Innokas Yhtymä Oy Vital Signs Monitor

Medium level vulnerabilities: Cross-site Scripting, Improper Neutralization of Special Elements in Output Used by a Downstream Component.
https://us-cert.cisa.gov/ics/advisories/icsma-21-007-01

ICSA-21-007-01: Hitachi ABB Power Grids FOX615 Multiservice-Multiplexer

Critical level vulnerability: Improper Authentication.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-01

ICSA-21-007-02: Omron CX-One

High level vulnerabilities: Untrusted Pointer Dereference, Stack-based Buffer Overflow, Type Confusion.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-02

ICSA-21-007-03: **Eaton EASYsoft**
Medium level vulnerabilities: Type Confusion, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-03

ICSA-21-007-04: **Delta Electronics CNCSoft-B**
High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Untrusted Pointer Dereference, Type Confusion.
https://us-cert.cisa.gov/ics/advisories/icsa-21-007-04

ICSA-21-005-01: **Schneider Electric Web Server on Modicon M340**
Medium level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Classic Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-01

ICSA-21-005-02: **Panasonic FPWIN Pro**
High level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-02

ICSA-21-005-03: **GE Reason RT43X Clocks**
Critical level vulnerabilities: Code Injection, Use of Hard-coded Cryptographic Key.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-03

ICSA-21-005-04: **Red Lion Crimson 3.1**
High level vulnerabilities: NULL Pointer Dereference, Missing Authentication for Critical Function, Improper Resource Shutdown or Release.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-04

ICSA-21-005-05: **Delta Electronics DOPSoft**
High level vulnerabilities: Out-of-bounds Write, Untrusted Pointer Dereference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-05

ICSA-21-005-06: **Delta Electronics CNCSoft ScreenEditor**
High level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-005-06

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 2021, ICS-CERT hasn’t published alerts.

The previous alerts can be found at the following link:

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