2021. September, 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 cara@blackcell.hu.

List of Contents

ICS GOOD PRACTICES, RECOMMENDATIONS 2
ICS TRAININGS, EDUCATION 3
ICS CONFERENCES 6
ICS INCIDENTS 9
BOOK RECOMMENDATION 10
BLACK CELL RECOMMENDATIONS 11
ICS VULNERABILITIES 12
ICS ALERTS 19

ICS good practices, recommendations

Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems

There is a critical point in the security of critical infrastructures, the comprehensive risk assessment. There are many methodologies and best practices, standards which can help us to execute the risk assessment.

There is a publication, which is relatively old, wrote in 2012, but the topic is actual nowadays. The publication introduces the related security guidelines and best practices and give some useful risk assessment tools.

The publication described the CORAS framework and the objective of it:

- To develop a practical framework for risk analysis.
- To assess the applicability, usability, and efficiency of the framework; and
- To investigate its commercial viability.

The publication shows some examples, tables and diagrams to understand the framework. Risk assessment starts with asset identification, threat and vulnerability identification and analysis.

The challenge for the authors is the continual development of the SCADA and ICS system risk model.

Future plans include:

- Development of a risk simulation model that mimics the actual risks endemic to SCADA and ICS systems; and
- Expansion of the current risk model to include parameters representing additional assets, risks, and vulnerabilities.

If you interested in the ICS/SCADA risk assessment, this publication may give you some useful information.

Source and more information are available on the following link:

https://icscsi.org/library/Documents/White_Papers/Francia%20et%20al%20-%20Security%20Best%20Practices%20and%20Risk%20Assessment%20of%20SCADA%20and%20ICS.pdf

ICS trainings, education

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

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- Emerging Technologies: From Smartphones to IoT to Big Data Specialization
- CAD and Digital Manufacturing 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 - 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
  - 4-9. October 2021
  - 18-23. October 2021
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 11-15. October 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

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

CyberICPS 2021)

The goal of the 7th Workshop on The Security Of Industrial Control Systems & of Cyber-Physical Systems is the following:

Cyber-physical systems (CPS) are physical and engineered systems that interact with the physical environment, whose operations are monitored, coordinated, controlled and integrated by information and communication technologies. These systems exist everywhere around us, and range in size, complexity and criticality, from embedded systems used in smart vehicles, to SCADA systems in smart grids to control systems in water distribution systems, to smart transportation systems and plant control systems, engineering workstations, substation equipment, programmable logic controllers (PLCs), and other Industrial Control Systems (ICS). These systems also include the emerging trend of Industrial Internet of Things (IIoT) that will be the central part of the fourth industrial revolution.

As ICS and CPS proliferate, and increasingly interact with us and affect our life, their security becomes of paramount importance. CyberICPS intends to bring together researchers, engineers and governmental actors with an interest in the security of ICS and CPS in the context of their increasing exposure to cyber-space, by offering a forum for discussion on all issues related to their cyber security.

The main topics are the followings: Security governance, System and network security, Incident Response and Digital Forensics for ICS/CPS, Case studies.

Darmstadt, Germany; 4-8. October 2021

More details can be found on the following website:

https://www.ds.unipi.gr/cybericps2021/

Cyber Security for Critical Assets Summit

The CS4CA Europe Summit gives cyber security experts a platform to discuss the problems affecting the region's critical infrastructure community, and most importantly, how to solve them.

Over the past year we have seen more cyber attacks, more threats and more vulnerabilities facing our security systems. The Covid-19 pandemic has only acted as a catalyst for our increasing interconnectivity. Now more than ever, the skills, techniques and processes for securing both digital and physical assets must evolve quickly in order to continue to safeguard the critical assets and infrastructure that keep our society running.

As a result, the CS4CA summit will unite 100's of IT & OT security leaders from across Europe's critical infrastructures, for 2-days of in-depth knowledge exchange, strategy planning and insight building online on 12th – 13th October.

Virtual event; 12-13. October 2021

More details can be found on the following website:

https://europe.cs4ca.com/

Industrial Control Systems (ICS) Cyber Security Conference

SecurityWeek's 2021 ICS Cyber Security Conference will be held at the InterContinental Atlanta with content available online as a hybrid event in SecurityWeek's virtual conference environment.

SecurityWeek's ICS Cyber Security Conference is the conference where ICS users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyse their causes and cooperate on solutions. Since its first edition in 2002, the conference has attracted a continually rising interest as both the stakes of critical infrastructure protection and the distinctiveness of securing ICSs become increasingly apparent.

Atlanta + Virtual (Hybrid); 26.28. October 2021

More details can be found on the following website:

https://www.icscybersecurityconference.com/

Public Safety Canada 2021 ICS Security Symposiums

As COVID-19 has forced many programs to shift their delivery model, and in the interest of the well-being of the presenters and attendees, the ICS Security Symposium will be held virtually until further notice.

Additionally, in order to ensure that the content is delivered in more practical segments, the 2021 conference will be split into four, themed, mini-conferences. Through each mini-conference, participants will view focused presentations and take part in group discussions on a given theme.

Technical Workshops:

Public Safety Canada's ICS Security technical workshops are focused on the development of basic incident handler skills for the ICS environment. The objective of this training is to raise awareness by giving a hands-on experience using real tools and targets. Participants will be expected to have a basic to moderate level of computer security training and proficiency within a networked environment.

Details on the next ICS Technical Workshop will be posted as it becomes available.

ICS Webinars:

Public Safety Canada hosts ICS-themed webinars that bring together various experts and industry leaders to present on in-depth and timely topics related to ICS and cyber security. It allows PS to

engage with stakeholders continuously throughout the year as well as provide opportunities to update the community on security topics, promote the ICS Symposium, and build relationships with experts and industry leaders.

Virtual event (until further notice); 25. 27. October 2021

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/index-en.aspx

ICCSICS002 2021

15. International Conference on Cyber Security of Industrial Control Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Security of Industrial Control Systems. 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 Cyber Security of Industrial Control Systems.

Paris, France; 28-29. October 2021

More details can be found on the following website:

https://waset.org/cyber-security-of-industrial-control-systems-conference-in-october-2021-in-paris

ICS incidents

14 Major SCADA Attacks and What You Can Learn From Them

On DPS telecom's website, you can find a very useful article about what happened with the SCADA systems in the past. The description of the 14 major SCADA attack's introduction is instructive and can help the operators to update their risk assessment process.

The 14 major SCADA attacks are the followings:

- Stuxnet,
- Night Dragon,
- Duqu, Flame, and Gauss,
- Shamoon - Saudi Aramco and RasGas,
- Target Stores,
- New York Dam,
- Havex,
- German Steel Mill,
- BlackEnergy,
- Ukraine Power Grid,
- "Kemuri" Water Company,
- Second Attack on the Ukraine Power Grid,
- CRASHOVERRIDE or Industroyer,
- SamSam,
- The Bottom Line,

Source and more details can be found on the following website:

https://www.dpstele.com/blog/major-scada-hacks.php

In 2018. Waterfall Security Solution published the Top 20 cyberattacks on Industrial Controls Systems paper, which is also a good analysis in this issue.

This publication shows the attacks sophistication and the consequences. This document is very useful to analyse our operational risks.

The publication is available at the following link:

https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf

Book recommendation

OT/ICS Cybersecurity

The book contains 7 very interesting article, from the experts of the ICS/OT world. The articles are the followings:

- Closing the IoT Security Gaps in your ICS
- From Warehouse to Enterprise with Edge Computing
- Open Secure Remote Operations: A Vision Fulfilled
- Secure Industrial Control Systems with Configuration Control
- Cybersecurity Using ICS ATT&CK Strategies
- Can a Solution Provider Handle Industrial Cybersecurity?
- Essential Start to Securing OT Systems: Risk Assessment

If you want to read this book, you can download it from the link. There are many useful recommendations and case studies in it.

Authors/Editors: Renee Bassett, Patrick Bedwell, Josh Eastburn, Albert Rooyakkers, Michael Rothschild, Jacob Chapman, Felipe Sabino Costa, Mark Hellinghuizer

Year of issue: 2021.

The book is available at the following link:

https://www.automation.com/en-us/assets/ebooks/automation-2021-ot-ics-cybersecurity

Black Cell recommendations

A brief look at the statistics about ICS ransomware attacks

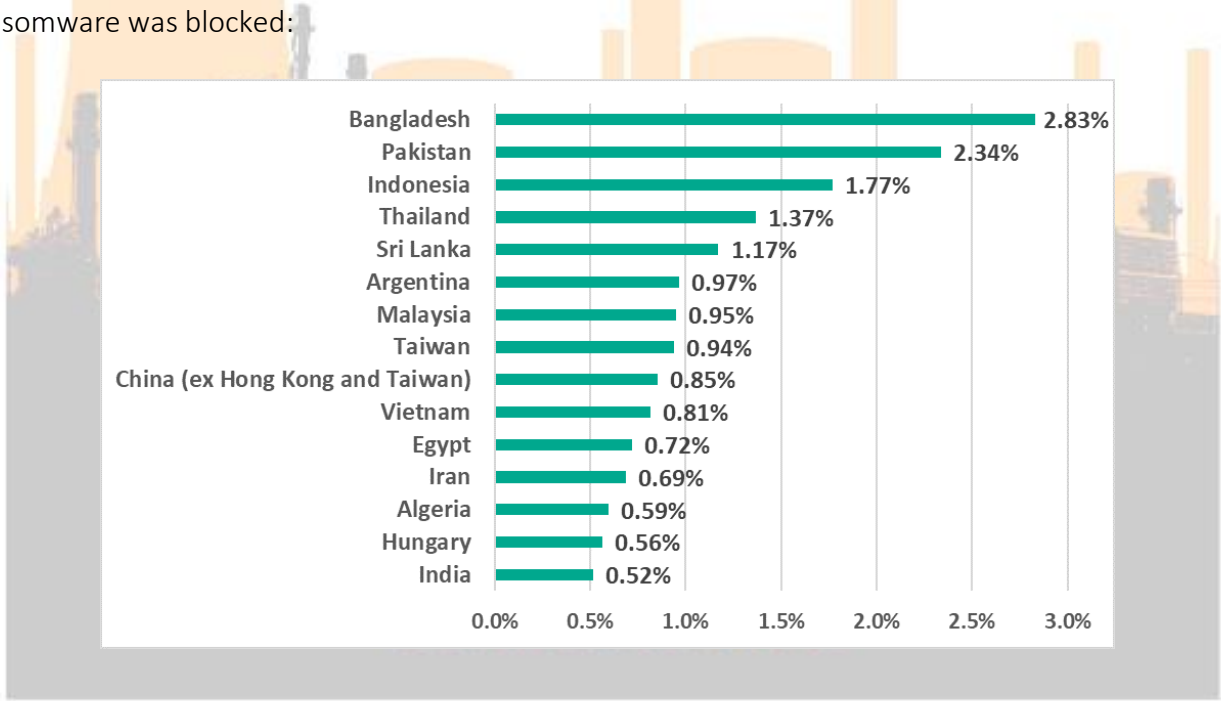
There are many ICS ransomware statistics, which try to show the threat landscape. One of them is the "Threat landscape for industrial automation systems. Statistics for H2 2020" from Kaspersky.

The statistics can give information about the numbers of ransomware attacks against the industrial control and/or automation systems, and other related and interesting data.

The number of attacks is ever-growing. According to the Kaspersky statistics in 2020, globally, the percentage of attacked ICS computers in the second half of the year was 33.4%, which was 0.85 percentage points higher than the first half of the year.

This trend is not surprising, from time to time this growth is predictable.

Let's see a statistic from the top 15 countries ranked by percentage of ICS computers on which ransomware was blocked:



Hungary is 14th in this list. The statistics generally reflect reality, therefore Hungarian ICS operators must be prepared for ransomware attacks, because they are targeted.

Other statistics may draw attention to other things and threats.

So, look for the statistics and draw conclusions as risks always vary according to statistics.

Source and more information are available at the following link:

https://ics-cert.kaspersky.com/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/#_Toc66285869

ICS vulnerabilities

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

ICSA-21-266-02: **Trane Tracer**
Critical level vulnerability: Code Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-266-02

ICSA-21-054-04: **Ovarro TBox (Update A)**
High level vulnerabilities: Code Injection, Incorrect Permission Assignment for Critical Resource, Uncontrolled Resource Consumption, Insufficiently Protected Credentials, Use of Hard-coded Cryptographic Key, Relative Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-04

ICSA-21-259-01: **Siemens RUGGEDCOM ROX**
High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Execution with Unnecessary Privileges, Improper Handling of Insufficient Permissions or Privileges.
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-01

ICSA-21-259-02: **Schneider Electric EcoStruxure and SCADAPack**
High level vulnerability: Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-02

ICSA-21-257-01: **Digi PortServer TS 16**
Critical level vulnerability: Improper Authentication.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-01

ICSA-21-257-02: **Johnson Controls Sensormatic Electronics KT-1**
High level vulnerability: Authentication Bypass by Capture-replay.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-02-0

ICSA-21-257-03: **Schneider Electric Struxureware Data Center Expert**
Critical level vulnerabilities: OS Command Injection, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-03

ICSA-21-257-04: **Siemens Simcenter Femap**
Law level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-04

ICSA-21-257-05: **Siemens Simcenter STAR-CCM+ Vieweri**
High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-05

ICSA-21-257-06: Siemens SIMATIC CP
Medium level vulnerability: Cleartext Storage of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-06

ICSA-21-257-07: Siemens APOGEE and TALON
Critical level vulnerability: Classic Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-07

ICSA-21-257-08: Siemens Teamcenter
High level vulnerabilities: Privilege Defined with Unsafe Actions, Authorization Bypass Through User-Controlled Key, Improper Restriction of XML External Entity Reference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-08

ICSA-21-257-09: Siemens NX
High level vulnerabilities: Use After Free, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-09

ICSA-21-257-10: Siemens SIPROTEC 5 relays
Critical level vulnerability: Classic Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-10

ICSA-21-257-11: Siemens SIMATIC RFID
High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-11

ICSA-21-257-12: Siemens SINEMA Server
Law level vulnerability: Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-12

ICSA-21-257-13: Siemens LOGO! CMR and SIMATIC RTU 3000
Medium level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-13

ICSA-21-257-14: Siemens SINEC NMS
High level vulnerabilities: Path Traversal, Cross-site Request Forgery.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-14

ICSA-21-257-15: Siemens SIMATIC NET CP Modules
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-15

ICSA-21-257-16: Siemens SIPROTEC 5
High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-257-16

ICSA-21-257-17: **Siemens Desigo CC Family**

Critical level vulnerability: Deserialization of Untrusted Data.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-17

ICSA-21-257-18: **Siemens Siveillance OIS**

Critical level vulnerability: OS Command Injection.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-18

ICSA-21-257-19: **Siemens SINEMA Remote Connect Server**

High level vulnerabilities: Modification of Assumed-Immutable Data, Improper Access Control, Exposure of Sensitive Information to an Unauthorized Actor, Improper Control of Interaction Frequency.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-19

ICSA-21-257-20: **Siemens LOGO! CMR and SIMATIC RTU 3000**

High level vulnerabilities: Incorrect Calculation of Buffer Size, Improper Certificate Validation.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-20

ICSA-21-257-21: **Siemens Industrial Edge**

Critical level vulnerability: Authorization Bypass Through User-controlled Key.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-21

ICSA-21-257-22: **Siemens Teamcenter Active Workspace**

Law level vulnerability: Path Traversal.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-22

ICSA-21-257-23: **Siemens SIMATIC and TIM**

Medium level vulnerability: Incorrect Authorization.

https://us-cert.cisa.gov/ics/advisories/icsa-21-257-23

ICSA-21-222-03: **Siemens JT2Go and Teamcenter Visualization** (Update A)

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Write, Out-of-bounds Read.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-03

ISCA-21-222-09: **Siemens SIMATIC S7-1200** (Update A)

High level vulnerability: Improper Authentication.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-09

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

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://us-cert.cisa.gov/ics/advisories/icsa-21-217-01

ICSA-21-194-03: Siemens PROFINET Devices (Update A)
High level vulnerability: Allocation of Resources Without Limits or Throttling.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-03

ICSA-21-194-06: Siemens SIMATIC Software Products (Update A)
High level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-06

ICSA-21-194-13: Siemens SINAMICS PERFECT HARMONY GH180 (Update A)
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-13

ICSA-21-194-17: Siemens SINUMERIK ONE and SINUMERIK MC (Update A)
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-17

ICSA-21-152-01: Siemens SIMATIC S7-1200 and S7-1500 CPU Families (Update A)
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-152-01

ICSA-21-131-03: Siemens Linux-based Products (Update D)
High level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-03

ICSA-21-131-12: Siemens SIMATIC SmartVNC HMI WinCC Products (Update A)
Critical level vulnerabilities: Access of Memory Location After End of Buffer, Improper Handling of Exceptional Conditions, Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-12

ICSA-21-103-07: Siemens Web Server of SCALANCE X200 (Update A)
Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-07

ICSA-21-068-10: Siemens SCALANCE and SIMATIC libcurl (Update B)
High level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10

ICSA-21-040-05: Siemens TIA Administrator (Update A)
High level vulnerability: Improper Access Control.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-05

ICSA-21-012-02: Siemens SCALANCE X Switches (Update B)

Critical level vulnerability: Use of Hard-coded Cryptographic Key.

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-02

ICSA-21-012-05: Siemens SCALANCE X Products (Update B)

Critical level vulnerabilities: Missing Authentication for Critical Function, Heap-based Buffer Overflow.

https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05

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

High level vulnerability: Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-20-324-05

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

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

High level vulnerability: Resource Exhaustion.

https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-04: Siemens PROFINET-IO Stack (Update E)

High level vulnerability: Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04

ICSA-19-253-03: Siemens Industrial Products (Update O)

High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03

ICSA-19-225-03: Siemens SCALANCE X Switches (Update C)

High level vulnerability: Insufficient Resource Pool.

https://us-cert.cisa.gov/ics/advisories/icsa-19-225-03

ICSA-21-252-01: AVEVA PCS Portal

High level vulnerability: Uncontrolled Search Path Element.

https://us-cert.cisa.gov/ics/advisories/icsa-21-252-01

ICSA-21-252-02: Delta Electronics DOPSoft 2

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

https://us-cert.cisa.gov/ics/advisories/icsa-21-252-02

ICSA-21-252-03: Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU

Critical level vulnerabilities: OS Command Injection, Improper Access Control, Cross-site Scripting, Use of Hard-coded Credentials, Unprotected Storage of Credentials, Incorrect Default Permissions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-252-03

ICSA-20-245-01: Mitsubishi Electric Multiple Products (Update C)

High level vulnerability: Predictable Exact Value from Previous Values.
https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01

ICSA-21-250-01: Mitsubishi Electric MELSEC iQ-R Series

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Insufficiently Protected Credentials, Overly Restrictive Account Lockout Mechanism.
https://us-cert.cisa.gov/ics/advisories/icsa-21-250-01

ICSA-21-250-02: Hitachi ABB Power Grids System Data Manager

Medium level vulnerability: Cleartext Storage of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsa-21-250-02

ICSA-21-245-01: Johnson Controls Sensormatic Electronics Illustra

High level vulnerability: Off-by-one Error.
https://us-cert.cisa.gov/ics/advisories/icsa-21-245-01

ICSA-21-245-02: JTEKT TOYOPUC Products

Low level vulnerability: Allocation of Resources Without Limits or Throttling.
https://us-cert.cisa.gov/ics/advisories/icsa-21-245-02

ICSA-21-245-03: Advantech WebAccess

Critical level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-245-03

ICSA-21-243-01: Sensormatic Electronics KT-1

No vulnerability level information: Use of Unmaintained Third-party Components.
https://us-cert.cisa.gov/ics/advisories/icsa-21-243-01

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

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-21-238-01: Johnson Controls Controlled Electronic Management Systems CEM Systems AC2000

High level vulnerability: Improper Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-238-01

ICSA-21-238-02: **Annke Network Video Recorder**

Critical level vulnerability: Stack-based Buffer Overflow.

https://us-cert.cisa.gov/ics/advisories/icsa-21-238-02

ICSA-21-238-03: **Delta Electronics DIAEnergie**

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.

https://us-cert.cisa.gov/ics/advisories/icsa-21-238-03

ICSA-21-238-04: **Delta Electronics DOPSoft**

High level vulnerability: Stack-based Buffer Overflow.

https://us-cert.cisa.gov/ics/advisories/icsa-21-238-04

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 September 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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