2021. February, 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

Security checklist of ICS/SCADA systems

The English National Cyber Security Centre (Ministry of Security and Justice) published a checklist in 2016, which can help to determine to the ICS/SCADA operators, whether their ICS/SCADA systems are sufficiently protected or not.

The target audience are the owners and administrators of ICS/SCADA systems and building management systems. The authors mentioned in the document, that the ICS/SCADA security improvements must based on risk assessment.

The checklist contains 7 organisational measures and 10 technical and operational measures with explanation and references. The reference list contains many good practices, standards and recommendations, which are very useful, if the organization wants to establish a robust cyber resilient ICS/SCADA security.

It's a very good collection of measures, briefly contains the most critical ICS/SCADA security and safety controls with implementation tips.

If an organization use this checklist as an audit controls list, the results can show the maturity level of the ICS/SCADA security. After the audit, the organization can focus on the critical points to improve the security.

The factsheet is available on the following link:

https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-checklist-security-of-ics-scada-systems

You can find more interesting publications on the National Cyber Security Centre's website:

https://english.ncsc.nl/publications

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in February 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 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
  - 08-13. March 2021.
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 08-12. March 2021.
  - 15-19. March 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:

- 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/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a 3 Days Course, which 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 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 March 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

Control Systems CyberSec USA Virtual Conference

The 7th Cyber Senate Control System Cyber Security USA conference will take place virtually March 29, 30, 31st EST online and LIVE in September 2021. Over 15 key presentations addressing threats to industrial organisations spanning Maritime, Nuclear, Rail, SmartGrid, Water, Engineering, Utility, Cloud, IOT, Telecom moderated by Global Cyber security Subject Matter Experts.

New focus streams on Industry 4.0 adoption, next generation technologies and how they be secured and utilised to gain competitive advantage. Participants can hear how IT/OT has already converged for many sectors, how they are managing IP enabled hardware and reconfiguring their divisions.

(Online); 29-31. March 2021.

More details can be found on the following website:

https://industrialcontrolcybersecusa.com/

Africa ICS Cybersecurity Conference and Expo

Africa ICS Cybersecurity Conference and Expo presents the B2B and B2C networking opportunity. The programme contains many interesting presentations, where the participants get to know the African ICS/SCADA systems and the African Women in Cybersecurity Forum.

In the conference you will find top level government officials, Private sector CEOs, Researchers and Innovators. Meaning the event is a crucial opportunity for buyers, vendors and experts to attend.

Nairobi, Kenya; 16-19. March 2021.

More details can be found on the following website:

https://10times.com/africaicscybersecurityconference

IFIP WG 11.10 International Conference on Critical Infrastructure Protection

The 15th annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will held in Arlington, Virginia. The following topics will be addressed in the conference: Infrastructure vulnerabilities, threats and risks, Infrastructure protection, Industrial control systems/SCADA security, Security challenges, solutions and implementation issues, Infrastructure sector interdependencies and security implications, Risk analysis, risk assessment and impact assessment methodologies, Modeling and simulation of critical infrastructures, Legal, economic, policy and human factors issues related to critical infrastructure protection, Secure information sharing, Case studies.

Arlington, Virginia (USA); 15-16. March 2021.

More details can be found on the following website:

http://www.ifip1110.org/

Cyber Supply Chain Risk Management (SCRM) and its impact information and Operational Technology (IT/OT)

This Zoom conference promises to be extremely interesting, because the speaker Mr. Randall Brooks presents Cyber Supply Chain Risk Management, which affected also the information and the operational technology. Nowadays this is a very hot topic all over the world.

Zoom (online); 03. March 2021.

More details can be found on the following website:

https://www.cerias.purdue.edu/news_and_events/events/security_seminar/details/index/13ah4gt7ncolbi44nhe1395h7b

ICS incidents

Ransomware attack against a packaging company's IT and OT systems

WestRock suffered a very high impacted ransomware attack at the end of January 2021. The attack also affected the Information and the Operational Technology of its infrastructure.

The company reported the incident to the law enforcement, and announced to the public, customers, partners etc.

The company working to maintain the business operations, but there were many problems, for example the connection between the company and the customers were only available on phones at this time.

The company didn't detail the operational technology problems. The only information about the OT, that this was affected in the ransomware attack.

WestRock initiated cyber security firms to handle the security incident and informed the public that activated the corporational business continuity plan.

More details can be found on the following websites:

https://www.securityweek.com/packaging-giant-westrock-says-ransomware-attack-impacted-ot-systems

https://ir.westrock.com/press-releases/press-release-details/2021/WestRock-Reports-Ransomware-Incident/default.aspx

https://www.databreaches.net/westrock-reports-ransomware-incident/

Author: the 2021 predictions about the cyber security challenges described that ransomware continue to be the biggest threat to organizations. These forecasts were true.

The incident is reached a high volume, and the company needed time to restore all of the processes and also the infrastructure.

Source: https://industrialcyber.co/threats-attacks/ransomware/westrock-faces-ransomware-incident-on-its-it-ot-systems/

A water supply system hacked in Oldsmar, Tampa

In February 2021, an attacker hacked the water supply system in Oldsmar, Tampa. The hacker tried to poison the people in Oldsmar. The attacker modified (increased) the amount of sodium hydroxide in Oldsmar's water treatment system, but a worker detected the malicious event, and set back the normal level of sodium hydroxide.

At first the water supply system operator thought, that the remote worker was his boss, who sometimes login, and take some actions in the system. In this case, the operator saw, that the sodium hydroxide modification was malicious, and the modifier wasn't his boss.

If the operator didn't detect this action, the following control process can detect the non-compliance of the amount of sodium hydroxide. The modification may cause catastrophic events in the city, but only a few days later, because the lead time is about 1-2 days.

After the event the Secret Service and FBI cyber units are trying to determine who is behind the hack and whether it was someone in the U.S. or overseas. It occurred just two days before the world's largest sport event, Super Bowl in a city about 30 miles away from Raymond James Stadium.

The water supply systems are critical infrastructure all over the world. If some hacking activity occurs, the lives of thousands of people can be in danger. The industrial systems cyber security is a priority in every country. This event can be detected if the defense-in-depth security is working and the disasters can be avoided.

The most important is to find the cause of the water supply systems' failure, which enabled the possibility of the attack, and to correct its errors.

More details can be found on the following websites:

https://www.cbsnews.com/news/florida-water-hack-oldsmar-treatment-plant/

https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html

Book recommendation

Securing SCADA systems

The Securing SCADA systems book is relatively old, published in 2005, but it's a recommended read, because this way the reader can identify the gaps between nowadays SCADA security and the 2005th SCADA security.

Krutz discusses the harsh reality that natural gas pipelines, nuclear plants, water systems, oil refineries, and other industrial facilities are vulnerable to a terrorist or disgruntled employee causing lethal accidents and millions of dollars of damage and also, what can be done to prevent this from happening.

Examines SCADA system threats and vulnerabilities, the emergence of protocol standards, and how security controls can be applied to ensure the safety and security of our national infrastructure assets.

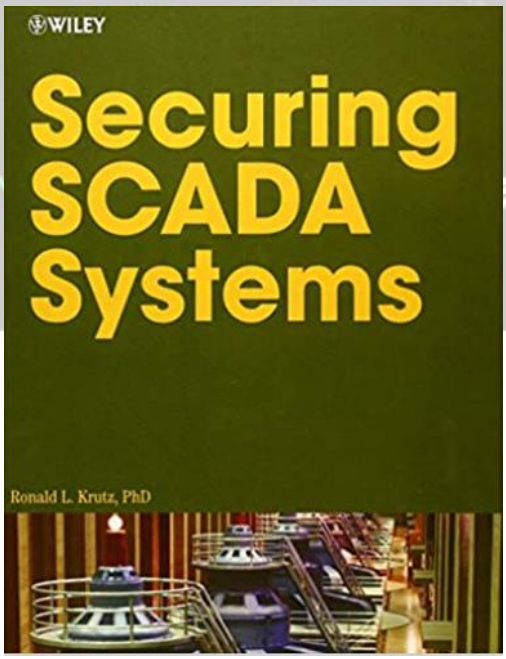
Some operators may realize while reading the book that they still have the same safety and security issues, like 15 years ago.

Authors/Editors: Ronald L. Krutz Phd.

Year of issue: 2005.

The book available at the following link:

https://www.amazon.com/Securing-SCADA-Systems-Ronald-Krutz/dp/0764597876



Black Cell recommendations

ICS system hardening

ICS/SCADA system hardening is a technique, that can help to build a more resilient security. Nowadays there are many good practices of hardening, and many of them are very useful.

Centre for the Protection of National Infrastructure from London, published a good practice guide, which is not only contains the hardening good practices. The reader can learn about it how to implement security architecture, how important the human background check, or how well is the management of third-party risks. The principles are detailed in the document, and there are many useful tips ons how to improve our ICS/SCADA process control and security.

The mentioned system hardening good practices are the followings:

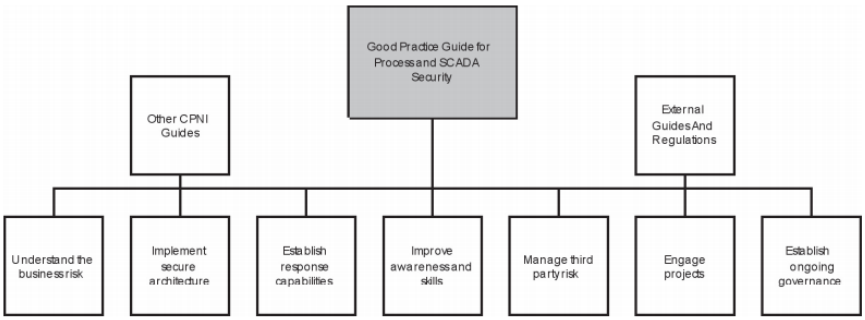
- Undertake hardening of process control systems to prevent network-based attacks. Remove or disable unused services and ports in the operating systems and applications to prevent unauthorised use.
- Understand what ports are open and what services and protocols are used by devices (especially embedded devices such as PLCs and RTUs). This could be established by a port scan in a test environment. All unnecessary ports and services should be disabled (e.g. embedded web servers).
- Ensure all in-built system security features are enabled.
- Restrict the use of removable media where possible (e.g. CDs, floppy disks, USB memory sticks etc.) and if possible removable media should not be used. Where it is necessary to use removable media then procedures should be in place to ensure that these are checked for malware prior to use.

System hardening is very important both in IT and OT. Without using hardening techniques, the exploitation of vulnerabilities is very easy. If the organization hardened the ICS/SCADA system, attackers doesn't have an easy way to earn their objectives.

The good practice is available at the following link:

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

Themes from the guide:



ICS vulnerabilities

In February 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-21-056-01: **PerFact OpenVPN-Client**

High level vulnerabiliy: External Control of System or Configuration Setting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-01

ICSA-21-056-02: **Fatek FvDesigner**

High level vulnerabilities: Use After Free, Access of Uninitialized Pointer, Stack-based Buffer Overflow, Out-of-Bounds Write, Out-of-Bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-02

ICSA-21-056-03: **Rockwell Automation Logix Controllers**

Critical level vulnerability: Insufficiently Protected Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03

ICSA-21-056-04: **ProSoft Technology ICX35**

High level vulnerabiliy: Permissions, Privileges, and Access Controls.
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-04

ICSA-21-054-01: **Rockwell Automation FactoryTalk Services Platform**

Critical level vulnerability: Use of Password Hash with Insufficient Computational Effort.
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-01

ICSA-21-054-02: **Advantech BB-ESWGP506-2SFP-T**

Critical level vulnerability: Use of Hard-coded Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-02

ICSA-21-054-03: **Advantech Spectre RT Industrial Routers**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation, Cleartext Transmission of Sensitive Information, Improper Restriction of Excessive Authentication Attempts, Use of a Broken or Risky Cryptographic Algorithm, Use of Platform-Dependent Third-party Components.
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-03

ICSA-21-049-01: **Johnson Controls Metasys Reporting Engine (MRE) Web Services**

High level vulnerabiliy: Path traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-049-01

ICSA-21-049-02: **Mitsubishi Electric FA engineering software products**

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-21-042-01: **Multiple Embedded TCP/IP Stacks** (Update A)

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

ICSA-21-012-01: Schneider Electric EcoStruxure Power Build-Rapsody (Update A)
High level vulnerabiliy: Unrestricted Upload of File with Dangerous Type.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-01

ICSA-20-282-02: Mitsubishi Electric MELSEC iQ-R Series (Update B)
High level vulnerabiliy: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02

ICSMA-21-047-01: Hamilton-T1
Law level vulnerabilities: Use of Hard-coded Credentials, Missing XML Validation.
https://us-cert.cisa.gov/ics/advisories/icsma-21-047-01

ICSA-21-047-01: Open Design Alliance Drawings SDK
High level vulnerabilities: Stack-based Buffer Overflow, Type Confusion, Untrusted Pointer Dereference, Incorrect Type Conversion or Cast, Memory Allocation with Excessive Size Value.
https://us-cert.cisa.gov/ics/advisories/icsa-21-047-01

ICSA-21-047-02: Rockwell Automation Allen-Bradley Micrologix 1100
High level vulnerabiliy: Improper Handling of Length Parameter Inconsistency.
https://us-cert.cisa.gov/ics/advisories/icsa-21-047-02

ICSA-21-021-05: WAGO M&M Software fdtCONTAINER (Update B)
High level vulnerabiliy: Deserialization of Untrusted Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05

ICSA-21-042-01: Multiple Embedded TCP/IP stacks
High level vulnerabiliy: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-042-01

ICSA-21-042-02: Rockwell Automation DriveTools SP and Drives AOP
High level vulnerabiliy: Uncontrolled Search Path Element.
https://us-cert.cisa.gov/ics/advisories/icsa-21-042-02

ICSA-20-203-01: Wibu-Systems CodeMeter (Update E)
Critical level vulnerabilities: Buffer Access with Incorrect Length Value, Inadequate Encryption Strength, Origin Validation Error, Improper Input Validation, Improper Verification of Cryptographic Signature, Improper Resource Shutdown or Release.
https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01

ICSA-21-040-01: GE Digital HMI/SCADA iFIX
Medium level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-01

ICSA-21-040-02: Advantech iView

Critical level vulnerabilities: SQL Injection, Path Traversal, Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-02

ICSA-21-040-03: Siemens SINEMA Server & SINEC NMS
High level vulnerabiliy: Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-03

ICSA-21-040-04: Siemens RUGGEDCOM ROX II
Critical level vulnerabilities: Improper Input Validation, NULL Pointer Dereference, Out-of-Bounds Write, Insufficient Verification of Data Authenticity, Improper Certificate Validation, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-04

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

ICSA-21-040-06: Siemens JT2Go and Teamcenter Visualization
High level vulnerabilities: Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer overflow, Out-of-Bounds Write, Type Confusion, Untrusted Pointer Dereference, Incorrect Type Conversion or Cast.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-06

ICSA-21-040-07: Siemens SCALANCE W780 and W740
Law level vulnerability: Allocation of Resources Without Limits or Throttling.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-07

ICSA-21-040-08: Siemens SIMARIS configuration
Law level vulnerability: Incorrect Default Permissions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-08

ICSA-21-040-09: SIMATIC WinCC Graphics Designer
Medium level vulnerability: Authentication Bypass Using an Alternate Path or Channel.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-09

ICSA-21-040-10: Siemens DIGSI 4
High level vulnerabiliy: Incorrect Default Permissions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-040-10

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

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-21-012-05: Siemens SCALANCE X Products (Update A)
Critical level vulnerabilities: Missing Authentication for Critical Function, Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-012-05

ICSA-20-343-05: Siemens Embedded TCP/IP Stack Vulnerabilities–AMNESIA:33 (Update A)
Medium level vulnerability: Integer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

ICSA-20-252-07: Siemens Industrial Products (Update C)
Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

ICSA-20-196-05: Siemens UMC Stack (Update E)
Medium level vulnerabilities: Unquoted Search Path or Element, Uncontrolled Resource Consumption, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-105-04: Siemens Climatix (Update A)
Medium level vulnerabilities: Cross-site Scripting, Basic XSS.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-04

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update D)
High level vulnerabiliy: Resource Exhaustion.
https://us-cert.cisa.gov/ics/advisories/icsa-20-105-07

ICSA-20-042-02: Siemens Industrial Products SNMP Vulnerabilities (Update C)
High level vulnerabilities: Data Processing Errors, NULL Pointer Dereference.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-02

ICSA-19-283-01: Siemens Industrial Real-Time (IRT) Devices (Update E)
High level vulnerabiliy: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-01

ICSA-19-225-03: Siemens SCALANCE X Switches (Update B)
High level vulnerabiliy: Insufficient Resource Pool.
https://us-cert.cisa.gov/ics/advisories/icsa-19-225-03

ICSA-19-162-04: Siemens SCALANCE X (Update B)
High level vulnerabiliy: Storing Passwords in a Recoverable Format.
https://us-cert.cisa.gov/ics/advisories/ICSA-19-162-04

ICSA-21-035-01: Luxion KeyShot

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Insufficient UI Warning of Dangerous Operations, Untrusted Pointer Dereference, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01

ICSA-21-035-02: Horner Automation Cscape

High level vulnerabiliy: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-035-02

ICSA-21-021-05: WAGO M&M Software fdtCONTAINER (Update A)

High level vulnerabiliy: Deserialization of Untrusted Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-021-05

ICSA-21-033-01: Rockwell Automation MicroLogix 1400

High level vulnerabiliy: Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-033-01

ICSA-21-033-02: Siemens SIMATIC HMI Comfort Panels & SIMATIC HMI KTP Mobile Panels

High level vulnerabiliy: Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-033-02

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 February 2021, ICS-CERT hasn't published alerts.

The previous alerts can be found at the following link:

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