2021. June, 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

SCADA security best practices

Water and Waste Digest published an article, with the following title: 7 SCADA security best practices to consider right now. These practices aren't usually strictly SCADA-related, however could add to the holistic cyber security approach.

This is the list:

1. Diagram all network traffic
2. Encrypt any unencrypted connection
3. Invest in an Intrusion Detection System (IDS)
4. Consider a data diode
5. Determine your risk profile
6. Understand the options and the limits of software and hardware
7. Employ two-factor or multi-factor authorization (MFA/2FA) and single sign-on (SSO)

Consider a data diode is not a standard. This practice is applicable, if the network do not need outside data, and using a data diode only allows data to flow out of a network, therefore cutting off one major vector of attack.

Risk profile determination is a hard and complicated task. As the ICS incidents shows, ransomware threats affect every sector. The special risks are not always visible, so it is a time and effort consuming procedure.

Two- or multi-factor authorization is impossible in many legacy systems, but where the possibility is given, the setting is obligatory nowadays. If the multi-factor authorization is not possible, implement workaround controls to mitigate the risks.

This best practice collection gives an Ignition Security Hardening Guide to help the operators.

The source and more information are available on the following link:

https://www.wwdmag.com/scada-systems/7-scada-security-best-practices-consider-right-now

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in July 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
- Industrial IoT on Google Cloud Platform
- 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

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
  - 12-17. July 2021.
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 12.16. July 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 (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 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 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 July 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

Event: The Secret of Israeli Cyber Innovation

The Conference is addressing an Israeli cyber startup, but there is also a speaker, who is the the Chief Executive Officer of SCADAfence. His presentation will be interesting to the industrial control system operators as well as the IT operators.

Innovation is a key component to a secure OT security system, because of the legacy systems and the increased number of connectivity with IIoT.

Virtual conference; 28. July 2021.

More details can be found on the following website:

https://us-cert.cisa.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

ICICSCS 2021

The 15th International Conference on Industrial Control Systems Cyber Security is held in Singapore and is a conference for researchers, which provides an exceptional value for students, academics and industry researchers.

ICICSCS 2021 aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of ICS Cyber Security. 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 Industrial Control Systems Cyber Security.

Singapore, Singapore 05-06. July 2021.

More details can be found on the following website:

https://waset.org/industrial-control-systems-cyber-security-conference-in-july-2021-in-singapore

ICS incidents

JBS Foods shuts down production after cyber-attack

Nowadays, all of the critical infrastructure sectors suffer from cyber-attacks all over the world. In May 2021, JBS Foods, a leading food company and the largest meat producer globally suffered a large-scale cyber-attack. The cyber-attack affected the production in the United States, Australia, and Canada.

The business continuity, the supply chain processes and the production in many countries stopped. In the United States, FBI is investigating the incident and CISA is coordinating with the FBI to offer technical support to the company in recovering from the ransomware attack.

In Australia, the government helping bring back JBS systems online, because only the offline operation was working after the cyber-attack.

The transportation and billing processes also shut down, therefore the lack of meat and increasing meat prices will be predicted until manufacturing and shipping will be online.

The backup system was not affected by the attack according to the news and JBS said, they try to restore the operation as soon as possible.

According to the White House, the attack comes from Russia, but the hacker group does not appoint.

A ransomware attack happens in almost every month, which is affecting critical infrastructure operators globally. Many of the affected organizations paid ransom to the extortionists to give back the files or the control of the ICS systems.

In this case, the IT systems were shut down, what made the OT systems to shut down, due to the interconnectedness of systems and processes, spill-over effects must also be considered.

Sources and more details can be found on the following websites:

https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/

https://www.bleepingcomputer.com/news/security/us-russian-threat-actors-likely-behind-jbs-ransomware-attack/

Book recommendation

ICS/OT Ransomware in the Supply Chain: Learnings from attacks in 2020

The supply chain ransomware attacks are the hottest topic nowadays in the IT and OT operation.

This book presents the OT-based ransomware forks. After the introduction, the author describes the SolarWinds Orion / Sunburst breaches and some related details. It also contains targeted ransomware statistics, which are presents interesting numbers.

Andrew Ginter mentioned the cloud connectivity and IIoT relationships and the importance of these risks based on interconnection in this issue.

The book presents defensive solutions, for example software-based prevention, the software based and related IDS solutions, and unidirectional protection. The book evaluated the attacks and defences and describes the conclusions.

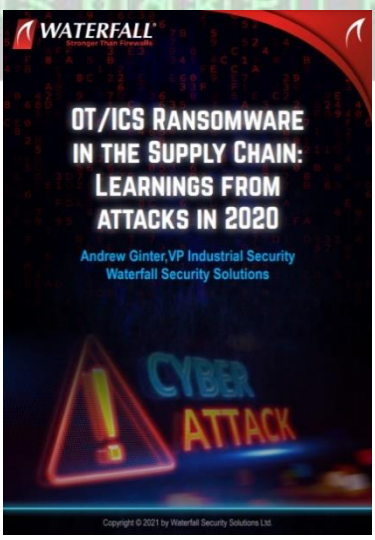
This book is very useful to the OT/ICS operation to evaluate the exposure of the ransomware landscape and the available security solutions in terms case of effectiveness.

Authors/Editors: Andrew Ginter

Year of issue: 2021.

The book available at the following link:

https://waterfall-security.com/ics-ot-ransomware-in-the-supply-chain-ebook/?utm_campaign=ICS%2FOT%20Ransomware%20in%20the%20Supply%20Chain%20eBook&utm_source=ppc&utm_medium=search%20ad&utm_term=ICS%2FOT%20Ransomware%20ebook&utm_content=11-feb-2021&utm_term=scada%20ransomware&utm_campaign=APAC%2BUK%2BAfrica+UGW+Grandma+Page&utm_source=adwords&utm_medium=ppc&hsa_acc=7472163176&hsa_cam=12347132057&hsa_grp=120554393689&hsa_ad=498749543440&hsa_src=g&hsa_tgt=kwd-1184025208984&hsa_kw=scada%20ransomware&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMI5Zmo05DB8AIViKiyCh1kKQXREAAYASAAEgL8P_D_BwE



Black Cell recommendations

ICS security podcasts

Nowadays many podcasts are available free on the Internet. The ICS and SCADA security podcasts are also available and usually the theme of the podcasts is very interesting.

Waterfall has a Podcast series, hosted by Andrew Ginter and Nate Nelson.

Some interesting episodes:

- Safe IT/OT integration with unidirectional security gateways
- Tips for recruiting and being recruited into industrial security positions – MEG DUBA | EPISODE #13
- Layer zero anomaly detection – ILAN GENDELMAN AND HADAS LEVINE | PODCAST EPISODE #19
- Targeted ransomware at a pharma plant – OFER SHAKED | EPISODE #37
- The industrial security podcast: risk assessment – understanding the problem
- Industrial cloud security – ANDREA CARCANO | EPISODE #50

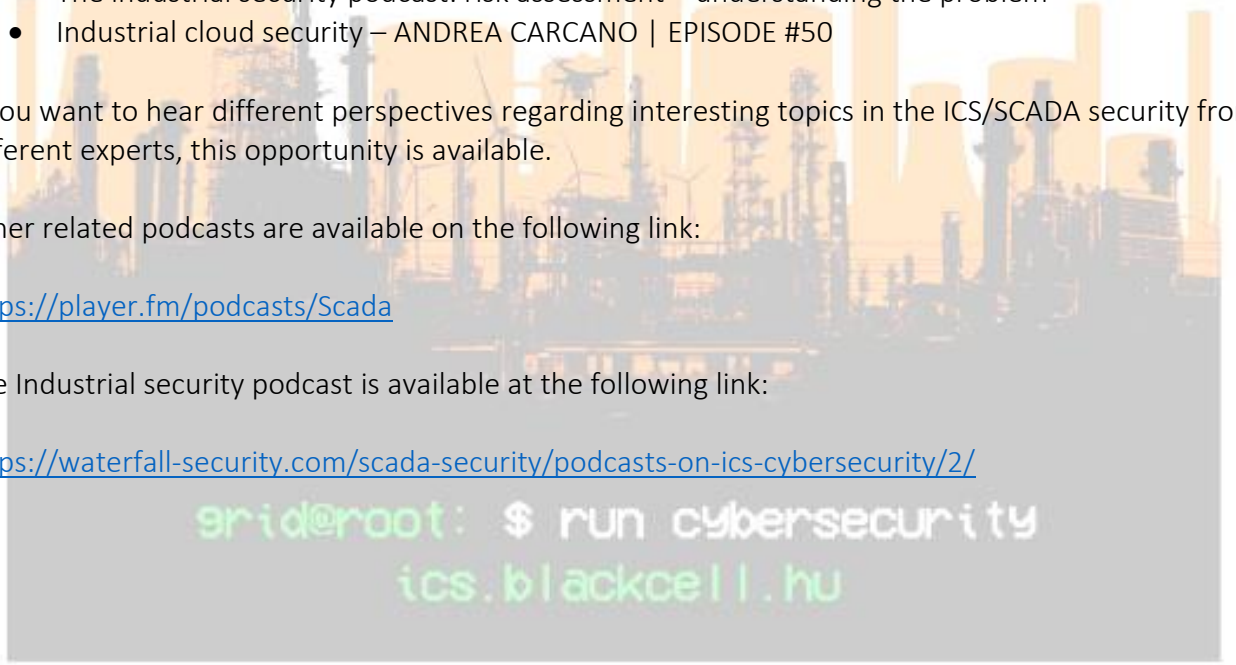
If you want to hear different perspectives regarding interesting topics in the ICS/SCADA security from different experts, this opportunity is available.

Other related podcasts are available on the following link:

https://player.fm/podcasts/Scada

The Industrial security podcast is available at the following link:

https://waterfall-security.com/scada-security/podcasts-on-ics-cybersecurity/2/



ICS vulnerabilities

In June 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-21-175-01: **Philips Interoperability Solution XDS**

Law level vulnerability: Clear Text Transmission of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsma-21-175-01

ICSA-21-175-01: **FATEK WinProladder**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-175-01

ICSA-21-173-01: **Advantech WebAccess HMI Designer**

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

ICSA-21-173-02: **CODESYS V2 web server**

Critical level vulnerabilities: Stack-based Buffer Overflow, Improper Access Control, Buffer Copy without Checking Size of Input, Improperly Implemented Security Check, Out-of-bounds Write, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-173-02

ICSA-21-173-03: **CODESYS Control V2 communication**

Critical level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-173-03

ICSA-21-173-04: **CODESYS Control V2 Linux SysFile library**

Medium level vulnerability: OS Command Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-173-04

ICSA-21-168-01: **Schneider Electric Enerlin'X Com'X 510**

High level vulnerability: Improper Privilege Management.
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-01

ICSA-21-168-02: **Softing OPC-UA C++ SDK**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-02

ICSA-21-168-03: **Advantech WebAccess/SCADA**

High level vulnerabilities: Open Redirect, Relative Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-168-03

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

High level vulnerability: Deserialization of Untrusted Data.

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

ICSA-20-280-01: Rockwell Automation ISaGRAF5 Runtime (Update A)

Critical level vulnerabilities: Use of Hard-coded Cryptographic Key, Unprotected Storage of Credentials, Relative Path Traversal, Uncontrolled Search Path Element, Cleartext Transmission of Sensitive Information.

https://us-cert.cisa.gov/ics/advisories/icsa-20-280-01

ICSA-21-166-01: ThroughTek P2P SDK

Critical level vulnerability: Cleartext Transmission of Sensitive Information.

https://us-cert.cisa.gov/ics/advisories/icsa-21-166-01

ICSA-21-166-02: Automation Direct CLICK PLC CPU Modules

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Cleartext Transmission of Sensitive Information, Unprotected Storage of Credentials.

https://us-cert.cisa.gov/ics/advisories/icsa-21-166-02

ICSMA-20-184-01: OpenClinic GA (Update B)

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Improper Restriction of Excessive Authentication Attempts, Improper Authentication, Missing Authorization, Execution with Unnecessary Privileges, Unrestricted Upload of File with Dangerous Type, Path Traversal, Improper Authorization, Cross-site Scripting, Use of Unmaintained Third-Party Components, Insufficiently Protected Credentials, Hidden Functionality.

https://us-cert.cisa.gov/ics/advisories/icsma-20-184-01

ICSMA-21-161-01: ZOLL Defibrillator Dashboard

Critical level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Use of Hard-coded Cryptographic Key, Cleartext Storage of Sensitive Information, Cross-site Scripting, Storing Passwords in a Recoverable Format, Improper Privilege Management.

https://us-cert.cisa.gov/ics/advisories/icsma-21-161-01

ICSA-21-161-01: Rockwell Automation FactoryTalk Services Platform

High level vulnerability: Protection Mechanism Failure.

https://us-cert.cisa.gov/ics/advisories/icsa-21-161-01

ICSA-21-161-02: AGG Software Web Server Plugin

High level vulnerabilities: Path Traversal, Cross-site Scripting.

https://us-cert.cisa.gov/ics/advisories/icsa-21-161-02

ICSA-21-159-01: Johnson Controls Metasys

High level vulnerability: Improper Privilege Management.

https://us-cert.cisa.gov/ics/advisories/icsa-21-159-01

ICSA-21-159-02: Open Design Alliance Drawings SDK

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Improper check for Unusual or Exceptional Conditions, Use After Free.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-02

ICSA-21-159-03: AVEVA InTouch
Medium level vulnerability: Clear Text Storage of Sensitive Information in Memory.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-03

ICSA-21-159-04: Schneider Electric IGSS
High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Access of Uninitialized Pointer, Use After Free, Release of Invalid Pointer or Reference, Improper Limitation of a Pathname to a Restricted Directory.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-04

ICSA-21-159-05: Schneider Electric Modicon X80
Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-05

ICSA-21-159-06: Thales Sentinel LDK Run-Time Environment
Critical level vulnerability: Incomplete Cleanup.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-06

ICSA-21-159-07: Siemens Mendix SAML Module
High level vulnerability: Insufficient Verification of Data Authenticity.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-07

ICSA-21-159-08: Siemens TIM 1531 IRC
High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-08

ICSA-21-159-09: Siemens Solid Edge
High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-09

ICSA-21-159-10: Siemens SIMATIC TIM libcurl
High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Improper Certificate Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-10

ICSA-21-159-11: Siemens SIMATIC NET CP 443-1 OPC UA
Critical level vulnerabilities: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer, Incorrect Calculation, Classic Buffer Overflow, Improper Authentication, Race Condition, Data Processing Errors, Exposure of Sensitive Information to an Unauthorized Actor, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11

ICSA-21-159-12: Siemens Simcenter Femap

High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-12

ICSA-21-159-13: Siemens SIMATIC RFID
High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-13

ICSA-21-159-14: Siemens JT2Go and Teamcenter Visualization
High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-159-14

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

ICSA-21-131-04: Siemens SINAMICS Medium Voltage Products Remote Access (Update A)
High level vulnerabilities: Improper Restriction of Operations Within the Bounds of a Memory Buffer, Access of Memory Location After End of Buffer, Uncontrolled Resource Consumption, Improper Initialization, Out-of-Bound Read, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Improper Null Termination.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-04

ICSA-21-103-06: Siemens Solid Edge File Parsing (Update A)
High level vulnerabilities: Out-of-bounds Write, Improper Restriction of XML External Entity Reference, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-06

ICSA-20-280-01: Rockwell Automation ISaGRAF5 Runtime
Critical level vulnerabilities: Use of Hard-coded Cryptographic Key, Unprotected Storage of Credentials, Relative Path Traversal, Uncontrolled Search Path Element, Cleartext Transmission of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/icsa-20-280-01

ICSA-20-252-06: Siemens SIMATIC HMI Products (Update A)
Medium level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Authentication Bypass by Primary Weakness.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-06

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

ICSA-20-161-04: Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update G)
Medium level vulnerability: Unquoted Search Path or Element.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

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

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

ICSA-17-339-01: Siemens Industrial Products (Update R)
High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01

ICSA-17-129-02: Siemens PROFINET DCP (Update T)
Medium level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

ICSA-21-154-01: Advantech iView
Critical level vulnerabilities: Missing Authentication for Critical Function, SQL Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-154-01

ICSMA-21-152-01: Hillrom Medical Device Management
Medium level vulnerabilities: Out-of-Bounds Write, Out-of-Bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsma-21-152-01

ICSA-21-152-01: Siemens SIMATIC S7-1200 and S7-1500 CPU Families
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

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 June 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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