2021. October, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents

ICS good practices, recommendations

Industrial control system (ICS) cybersecurity advice, best practices

In 2019 Osman Ahmed, Asad Rehman and Ahmed Habib wrote an article, where they give some good practices to increase ICS cybersecurity.

The best practice contains six common entry points for attacks, eight cybersecurity precautions for attacks by type, and four steps to improve.

Six common entry points for attackers are:

- Inbound attacks from external networks, internet, and remote connections through enterprise resource planning (ERP) software, gateways, and data and document repositories and online historians,
- Improperly configured firewalls and gateways,
- User access through stolen or phished credentials into business workstations and control computers,
- Physical attacks that target production systems, in most cases these are human-machine interfaces (HMIs), engineer and operator workstations, and actual process safety controllers,
- Lateral network attacks that target control networks and use industrial communication protocols to discover other devices on the network and spread malicious code,
- Social engineering attacks, which focus on using personally identifiable information to trick insiders into granting access, opening gateways and running scripts unintentionally.

Eight cybersecurity precautions:

1. Segregation and segmentation
2. Manage user access control
3. Patch frequently
4. Run validation checks
5. Add physical security
6. Train on cybersecurity
7. Create an incident response plan
8. Maintain an updated asset register

Four phases for a cybersecurity initiative:

Phase 1: Design and framework
Phase 2: Gap assessment
Phase 3: Implementation
Phase 4: Audit

Source and more information are available on the following link:

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

ICS trainings, education

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

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
  - 1-6. November 2021
  - 13-18. November 2021
  - 15-20. November 2021
  - 29. November – 4. December 2021
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 11-16. November 2021
  - 15-20. November 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 November 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

Annual Industrial Control Cyber Security Europe Conference

Annual Industrial Control Cyber Security Europe Conference will be dominated by the best global cyber security subject matter experts in the ICS domain, including executive leadership from utilities, water, oil and gas, aviation, rail, chemical, nuclear and maritime industries. The program will address the escalating cyber risk and resilience challenges associated with the adoption and convergence of operational technologies in enterprise facing architecture.

London, United Kingdom; 02. November 2021

More details can be found on the following website:

https://10times.com/industrial-control-security-europe

ICSICSCPS 2021

The 15. International Conference on Security of Industrial Control Systems and Cyber Physical 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 Security of Industrial Control Systems and Cyber Physical 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 Security of Industrial Control Systems and Cyber Physical Systems.

Some very interesting, selected papers from the program: A Medical Vulnerability Scoring System Incorporating Health and Data Sensitivity Metrics, Remote Monitoring and Control System of Potentiostat Based on the Internet of Things, Trusting Smart Speakers: Analysing the Different Levels of Trust between Technologies.

Cape Town, South Africa; 04-05. November 2021

More details can be found on the following website:

https://waset.org/security-of-industrial-control-systems-and-cyber-physical-systems-conference-in-november-2021-in-cape-town

16th Annual API Cybersecurity Conference For The Oil & Natural Gas Industry

For 16 years it has been the only cybersecurity conference dedicated to the oil and natural gas industry and has a loyal and dedicated attendee base. It is also volunteer-driven, both at the planning committee and speaker level. The conference consistently produces a compelling program, with a focus on safety, best practices, and innovation. In addition, the conference provides an opportunity

for attendees to earn CPEs (Continuing Professional Education), maintaining their certifications and required hours. Finally, the conference provides the opportunity for networking and idea exchange, with the dedicated sponsors and exhibitors sharing their latest products and services.

The Woodlands, Texas, USA and Virtual; 09-10. November 2021

More details can be found on the following website:

https://www.api.org/products-and-services/events/calendar/2021/cyber

Industrial Security Conference

The first international Industrial Security Conference in Copenhagen. During the 3 days programme, the participants can experience interesting keynotes, expert presentations, knowledge sharing and networking. Over the course of the conference, the participants will be updated on the current threat landscape and can learn from renowned experts who are sharing their knowledge on securing industrial control systems – such as SCADA, PLC and Distributed Control Systems.

There will be many interesting topics, for example: Network visibility considerations in industrial control system monitoring, the State of the Industrial Cybersecurity in Europe, Red Team/Blue Team playground – fun at the ICS range, cyber security in an offshore OT environment, Industrial Technology Trajectory: Running with Scissors, Top 20 Secure PLC Coding Practices, manufacturer challenges, how to cover and validate security requirements in tenders for your suppliers or bridging the gap between IT and OT.

Copenhagen, Denmark; 15-17. November 2021

More details can be found on the following website:

https://insightevents.dk/isc-cph/

ICS incidents

US critical infrastructure hit by ransomware in agricultural sector

In the United States, New Cooperative Inc. suffered a ransomware attack, which was disrupted the supply chain of human food and animal feeding schedules.

Some news said that the company paid for the extortioners, but the New Cooperative Inc. didn't confirmed this statement. The supply chain was only disrupted for a short time and the company found a workaround to maintain the business continuity.

Cybersecurity experts said that the entry point was weak passwords. From 120 employees more than 10 used the "chicken1" password.

The available information doesn't mention any other technical details, but it is very important, that where the companies' IT and OT systems are not fully segregated, the same incident can happen at any time.

In this situation we don't know that what systems crashed or what exactly means that the attack disrupted the supply chain. Therefore, the IT and OT security experts must secure both environments to maintain the business continuity.

Weak passwords are very big risks in IT and OT as well. The cyber security principles are very important besides the management and audit activities. Without these actions the cybersecurity will be compromised eventually.

"*President Biden has warned Russian President Putin that attacks on U.S. critical infrastructure, including the agriculture sector, will be met with a response, suggesting the nation could hit back with a cyber volley of its own. Perhaps recognizing that its attack on New Coop may reverberate beyond the single event, BlackMatter has posted on its website that it refrains from lining up critical infrastructure targets, even though to all appearances it apparently does.*"

The source and more information available at the following link:

https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/new-cooperative-ransomware-attack-timeline-status-updates/

https://www.reuters.com/technology/iowa-farm-services-company-reports-cybersecurity-incident-2021-09-20/

Book recommendation

Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment

The book is the second edition, the first edition was released in 2017. The book contains 5 sections, which are the followings:

- Introduction and recap of first edition,
- A modern look at the industrial control system architecture,
- The industrial demilitarized zone,
- Designing the ICS architecture with security in mind,
- Introduction to security monitoring.

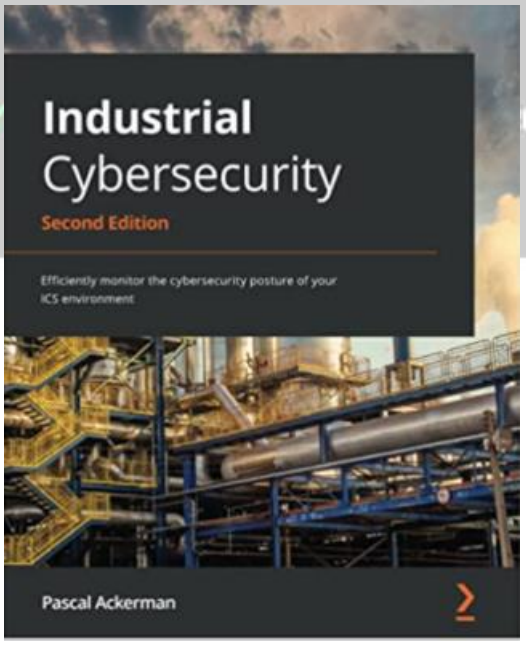
Things you will learn: monitor the ICS security posture actively as well as passively, respond to incidents in a controlled and standard way, understand what incident response activities are required in your ICS environment, perform threat hunting exercises using the Elasticsearch and Kibana stack, assess the overall effectiveness of your ICS cybersecurity program, discover tools, techniques methodologies and activities to perform risk assessments for your ICS environments.

Authors/Editors: Pascal Ackerman

Year of issue: 2021.

The book is available at the following link:

https://www.amazon.com/Industrial-Cybersecurity-Efficiently-cybersecurity-environment/dp/1800202091



Black Cell recommendations

Do you know Dale Peterson?

Dale Peterson has a blog, where every Friday he publishes some news and notes in the theme of ICS security. The blog contains every article from 2007 to nowadays.

This is the blog's website:

https://dale-peterson.com/blog/

These are some interesting articles from the near past:

- More OT Professionals Needed
- Sorry, Security Is A Cost
- Is IT/OT Convergence's Momentum Unstoppable?
- Universities Beginning To Offer ICS Security Courses and Degree Programs – More Needed
- Evaluating The ICS ATT&CK Evaluations
- ICS Security Buzzword Rankings
- It's Out! Top 20 Secure PLC Coding Practices
- 3 Incident Response Playbooks for OT
- How Do We Solve The OT Cybersecurity Staffing Challenges?
- Legacy System Problem Keeps Growing
- Women In ICS Security

and so on…

The articles show how complex the ICS security is, and how many related field has a great amount of problems.

Have a good browsing!

In this link, Dale Peterson give a short summary from ICS security:

https://www.youtube.com/watch?v=7NuLVJLOyW4

ICS vulnerabilities

In October 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-21-294-01: **B. Braun Infusomat Space Large Volume Pump**

Critical level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Cleartext Transmission of Sensitive Information, Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity, and Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsma-21-294-01

ICSA-21-294-01: **ICONICS GENESIS64 and Mitsubishi Electric MC Works64**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-294-01

ICSA-21-294-02: **Delta Electronics DIALink**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Cross-site Scripting, Improper Neutralization of Formula Elements in a CSV File, Cleartext Storage of Sensitive Information, Uncontrolled Search Path Element, Incorrect Default Permissions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-294-02

ICSA-21-294-03: **ICONICS GENESIS64 and Mitsubishi Electric MC Works64 OPC UA**

High level vulnerability: Uncontrolled Recursion.
https://us-cert.cisa.gov/ics/advisories/icsa-21-294-03

ICSA-21-292-01: **AUVESY Versiondog**

Critical level vulnerabilities: Improper Access Control, Incorrect Permission Assignment for Critical Resource, Use of Hard-coded Cryptographic Key, Out-of-bounds Read, Use After Free, Out-of-bounds Write, Write-what-where Condition, Use of Potentially Dangerous Function, Unrestricted Upload of File with Dangerous Type, External Control of File Name or Path, External Control of System or Configuration Setting, Improper Input Validation, Uncontrolled Resource Consumption, Uncontrolled Search Path Element, Authentication Bypass by Capture-replay, SQL Injection, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-292-01

ICSA-21-292-02: **Trane HVAC Systems Controls**

Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-292-02

ICSA-21-287-01: **Schneider Electric CNM**

High level vulnerability: Improper Privilege Management.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-01

ICSA-21-287-02: **Uffizio GPS Tracker**

Critical level vulnerabilities: Improper Access Control, Unrestricted Upload of File with Dangerous Type, Open Redirect, Cross-site Scripting, Cross-site Request Forgery.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-02

ICSA-21-287-03: Mitsubishi Electric MELSEC iQ-R Series
Critical level vulnerability: Authorization Bypass Through User-controlled Key.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-03

ICSA-21-287-04: Siemens SINUMERIK
High level vulnerability: Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-04

ICSA-21-287-05: Siemens SINEC NMS
High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory, Improper Authorization, Exposure of Sensitive Information to an Unauthorized Actor, Deserialization of Untrusted Data, Improper Neutralization of Special Elements used in an SQL Command.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-05

ICSA-21-287-06: Siemens Solid Edge
High level vulnerabilities: Use After Free, Out-of-bounds Read, Access of Uninitialized Pointer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-06

ICSA-21-287-07: Siemens SCALANCE
Critical level vulnerabilities: Cross-site Request Forgery, OS Command Injection, Classic Buffer Overflow, Command Injection, Path Traversal, Missing Encryption of Sensitive Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-07

ICSA-21-287-08: Siemens RUGGEDCOM ROX Devices
High level vulnerabilities: Improper Privilege Management, Execution with Unnecessary Privileges, Improper Handling of Insufficient Permissions or Privileges.
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-01

ICSA-21-287-09: Siemens SIMATIC Process Historian
Critical level vulnerability: Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-287-09

ICSA-21-259-01: Siemens RUGGEDCOM ROX (Update A)
High level vulnerabilities: Improper Privilege Management, Execution with Unnecessary Privileges, Improper Handling of Insufficient Permissions or Privileges.
https://us-cert.cisa.gov/ics/advisories/icsa-21-259-01

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

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

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

ICSA-21-131-03: Siemens Linux-based Products (Update E)
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 B)
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-21-131-14: Siemens SCALANCE W1750D (Update B)
Critical level vulnerabilities: Improper Authentication, Classic Buffer Overflow, Command Injection, Improper Input Validation, Race Condition, Cross-site Scripting, Basic XSS, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-14

ICSA-20-042-04: Siemens PROFINET-IO Stack (Update F)
High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04

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

ICSA-19-283-02: Siemens PROFINET Devices (Update K)
High level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-19-283-02

ICSA-19-085-01: Siemens SCALANCE X (Update C)
Medium level vulnerability: Expected Behavior Violation.
https://us-cert.cisa.gov/ics/advisories/ICSA-19-085-01

ICSA-17-339-01: Siemens Industrial Products (Update S)
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 U)
Medium level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

ICSA-21-285-01: Advantech WebAccess SCADA
Low level vulnerability: Missing Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-285-01

ICSA-21-285-02: Advantech WebAccess

Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-285-02

ICSA-21-285-03: Schneider Electric IGSS

Critical level vulnerabilities: Classic Buffer Overflow, Unrestricted Upload of File with Dangerous Type, Path Traversal, Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-285-03

ICSA-21-280-01: Johnson Controls exacqVision Server Bundle

Critical level vulnerability: Improper Privilege Management.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-01

ICSA-21-280-02: Mobile Industrial Robots Vehicles and MiR Fleet Software

Critical level vulnerabilities: Improper Access Control, Integer Overflow or Wraparound, Exposure of Resource to Wrong Sphere, Missing Authentication for Critical Function, Missing Encryption of Sensitive Data, Exposure of Sensitive Information to an Unauthorized Actor, Weak Encoding for Password, Incorrect Default Permissions, Failure to Handle Incomplete Element.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-02

ICSA-21-280-03: Johnson Controls exacqVision

High level vulnerability: Integer Overflow or Wraparound.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-03

ICSA-21-280-04: Mitsubishi Electric MELSEC iQ-R Series C Controller Module

Medium level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-04

ICSA-21-280-05: InHand Networks IR615 Router

Critical level vulnerabilities: Improper Restriction of Rendered UI Layers or Frames, Improper Authorization, Cross-site Request Forgery, Inadequate Encryption Strength, Improper Restriction of Excessive Authentication Attempts, Unrestricted Upload of File with Dangerous Type, Cross-site Scripting, OS Command Injection, Observable Response Discrepancy, Weak Password Requirements.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-05

ICSA-21-280-06: FATEK Automation WinProladder

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Unexpected Sign Extension, Stack-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use After Free.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-06

ICSA-21-280-07: FATEK Automation Communication Server

Critical level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-280-07

ICSA-21-278-01: Mitsubishi Electric GOT and Tension Controller

High level vulnerabilities: Improper Handling of Exceptional Conditions, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-278-01

ICSA-21-278-02: Emerson WirelessHART Gateway

High level vulnerabilities: Missing Authentication for Critical Function, Improper Input Validation, Improper Limitation of a Pathname to a Restricted Directory, Write-what-where Condition, Improper Neutralization of Special Elements used in an OS Command, Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-278-02

ICSA-21-278-03: Moxa MXview Network Management Software

Critical level vulnerabilities: Path Traversal, Use of Hard-coded Password, Unprotected Transport of Credentials, Injection, Improper Access Control.
https://us-cert.cisa.gov/ics/advisories/icsa-21-278-03

ICSA-21-278-04: Honeywell Experion PKS and ACE Controllers

Critical level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Relative Path Traversal, Improper Neutralization of Special Elements in Output Used by a Downstream Component.
https://us-cert.cisa.gov/ics/advisories/icsa-21-278-04

ICSMA-18-219-02: Medtronic MiniMed MMT-500/MMT-503 Remote Controllers (Update A)

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Authentication Bypass by Capture-replay.
https://us-cert.cisa.gov/ics/advisories/ICSMA-18-219-02

ICSMA-21-273-01: Boston Scientific Zoom Latitude

Medium level vulnerabilities: Use of Password Hash with Insufficient Computational Effort, Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques, Improper Access Control, Missing Support for Integrity Check, Reliance on Component That is Not Updateable.
https://us-cert.cisa.gov/ics/advisories/icsma-21-273-01

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 October 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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