2021. August, 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

SCADA security hack chat

There are many forums, where the experts always said, that the most important in cybersecurity is the information sharing. This phrase is true, but the information sharing is not sufficient many times.

Every organization wants to have information but is not interested in giving. This is a very big problem in the Critical Infrastructure sector, where knowing about a threat can be literally a question of life and death.

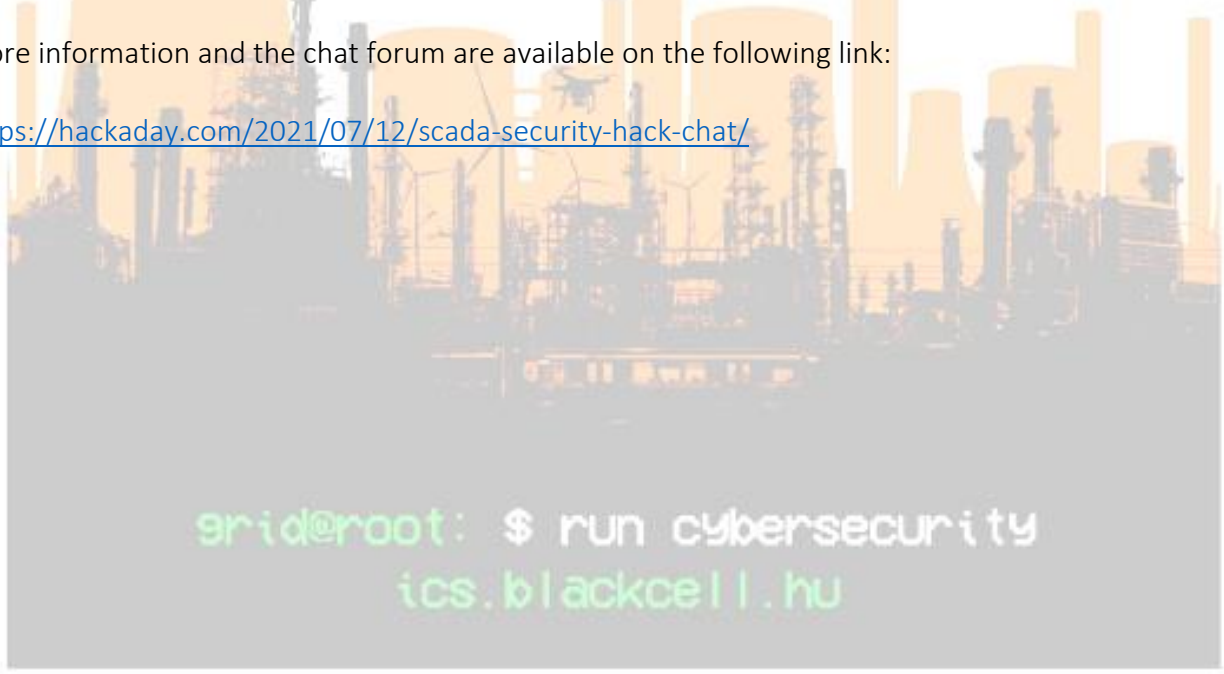
There is a platform, where the SCADA and OT security experts could share information regarding attacks and other security-related issues.

The SCADA security hack chat is an open platform, where the above possibilities are feasible.

If you agree the comment policy, you should use the platform, read and share information about the operational problems, security related issues, ongoing malware campaigns or other things.

More information and the chat forum are available on the following link:

https://hackaday.com/2021/07/12/scada-security-hack-chat/



ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in September 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
  - 20-25. September 2021
  - 27-02. September – October 2021
  - anytime, on demand.

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

Kaspersky Industrial Cybersecurity Conference 2021

This is the 9th International Conference organized by Kaspersky on Industrial Cybersecurity and is held in Russia. Industrial cybersecurity experts will attend to the conference from more than 20 countries.

Kaspersky Industrial Cybersecurity Conference is one of the leading conferences in the industrial cybersecurity area, gathering cybersecurity experts, researchers, industrial automation vendors, system integrators and customers from all over the world. During the conference, participants has the opportunity to discuss important issues, share their expertise and learn about new approaches to securely integrating information technology into industrial control systems.

Sochi, Russia; 8-10. September 2021

More details can be found on the following website:

https://ics.kaspersky.com/conference/

CS4CA USA Summit

Cyber Security for Critical Assets Summit will bring together 100's of IT & OT security leaders from across US critical infrastructure, for 2-days of in-depth knowledge exchange, strategy planning and insight building on September 16th-17th.

The summit's dynamic hybrid format offers two dedicated streams, allowing delegates to home in on their special areas of interest, as well as plenary sessions that binds groups of professionals, both in-person and online.

This is a unique opportunity to build partnerships with senior security professionals from the country's Oil & Gas, Energy, Utilities, Power, Water, Mining, Chemical and Pharmaceutical industries while participating in the discussions shaping the American cybersecurity landscape in 2021 and beyond.

Houston, Texas, USA; 16-17. September 2021

More details can be found on the following website:

https://usa.cs4ca.com/

International Conference on Industrial Control Systems Cyber Security

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

Lisbon, Portugal; 20-21. September 2021

More details can be found on the following website:

https://waset.org/industrial-control-systems-cyber-security-conference-in-september-2021-in-lisbon

ICS incidents

PwnedPiper critical bug set impacts major hospitals in North America

Ionut Ilascu wrote an article on Bleepingcomputer, where mentioned that Pneumatic tube system (PTS) stations used in thousands of hospitals worldwide are vulnerable to a set of nine critical security issues collectively referred to as PwnedPiper.

PTS solutions are critical in the life of hospitals, many processes are failed without PTS. The problem is that some critical bugs on the system left unpatched.

Research from Armis, a connected device security company, revealed that an unauthenticated attacker could gain full control over some TransLogic PTS stations connected to the internet and then could take over the entire PTS network of a target hospital.

The following vulnerabilities identified:

- CVE-2021-37163: two cases of always-active hardcoded passwords (user and root accounts), accessible over Telnet
- CVE-2021-37167: privilege escalation; using the hardcoded credentials, an attacker could run a user script with root privileges
- CVE-2021-37166: denial-of-service (DoS) caused by the GUI process of Nexus Control Panel binding a local service on all interfaces
- CVE-2021-37161 - Underflow in udpRXThread
- CVE-2021-37162 - Overflow in sccProcessMsg
- CVE-2021-37165 - Overflow in hmiProcessMsg
- CVE-2021-37164 - Off-by-three stack overflow in tcpTxThread
- CVE-2021-37160: unencrypted, unauthenticated firmware upgrades on the Nexus Control Panel. An attacker could leverage it to install malicious firmware on the system, essentially taking full control over it.

The firmware update fixes the most critical CVE-2021-37160 vulnerability. The other vulnerabilities are waiting for the updates.

Without the other patches the article gives the following recommendations to mitigate the risks:

- Block any use of Telnet (port 23) on the Translogic PTS stations (the Telnet service is not required in production)
- Deploy access control lists (ACLs), in which Translogic PTS components (stations, blowers, diverters, etc.) are only allowed to communicate with the Translogic central server (SCC).
- Use the following Snort IDS rule to detect exploitation attempts of CVE-2021-37161, CVE-2021-37162 and CVE-2021-37165

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

https://www.bleepingcomputer.com/news/security/pwnedpiper-critical-bug-set-impacts-major-hospitals-in-north-america/

Book recommendation

Cyber Security for Industrial Control Systems

From the Viewpoint of Close-Loop provides a comprehensive technical guide on up-to-date new secure defending theories and technologies, novel design, and systematic understanding of secure architecture with practical applications. The book consists of 10 chapters, which are divided into three parts. The first three chapters extensively introduce secure state estimation technologies, providing a systematic presentation on the latest progress in security issues regarding state estimation. The next five chapters focus on the design of secure feedback control technologies in industrial control systems, displaying an extraordinary difference from that of traditional secure defending approaches from the viewpoint of network and communication. The last two chapters elaborate on the systematic secure control architecture and algorithms for various concrete application scenarios.

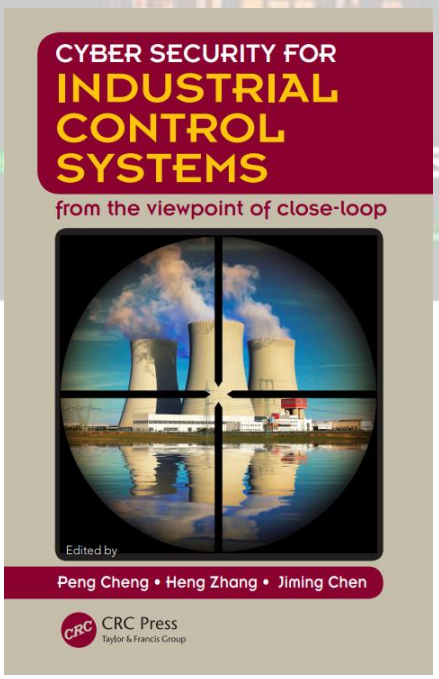
The authors provide detailed descriptions on attack model and strategy analysis, intrusion detection, secure state estimation and control, game theory in closed-loop systems, and various cyber security applications. The book is useful to anyone interested in secure theories and technologies for industrial control systems.

Authors/Editors: Peng Cheng, Heng Zhang, Jiming Chen

Year of issue: 2016

The book is available at the following link:

https://ebooks-it.org/1498734731-ebook.htm



Black Cell recommendations

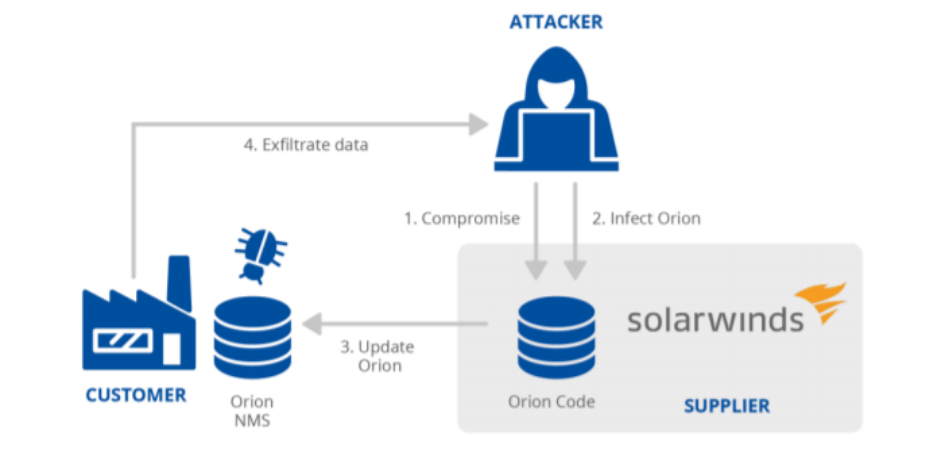
ENISA threat landscape for supply chain attacks

ENISA published a report last month, which introduces the supply chain attack threats and related incidents, conclusions, recommendations.

Many incidents happened nowadays, which are affected the supply chains all over the world, for example COVID-19 or the Evergreen Suez Canal blockage. These situations have negative effects to the supply chains and the business continuity.

Without these situations the attackers know that supply chain attacks are usually successful, because of the inappropriate security.

ENISA explains these attacks and introduces the lifecycle of these attacks. There are many techniques to compromise the customers. ENISA published the Solarwinds Orion situation in the report:



To understand them, ENISA analysed the flow of the attacks and in this analysis, more than 50% of the supply chain attacks were attributed to well-known cybercrime groups, including APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 and TA428.

The targets for these recommendations are the customers and the suppliers. Every process is vulnerable if the owners don't realize the threats and risks. One of the recommendations is the MITRE D3FEND framework, what can help to mitigate the supply chain risks.

The MITRE D3FEND framework is available at the following link:

https://d3fend.mitre.org/

Source and more information are available at the following link:

https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ICS vulnerabilities

In August 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-21-236-01: **Hitachi ABB Power Grids TropOS**

High level vulnerabilities: Injection, Inadequate Encryption Strength, Missing Authentication for Critical Function, Improper Authentication, Improper Validation of Integrity Check Value, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-236-01

ICSA-21-236-02: **Hitachi ABB Power Grids Utility Retail Operations and CSB Products**

High level vulnerability: Insufficiently Protected Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-236-02

ICSA-21-236-03: **Delta Electronics TPEditor**

High level vulnerability: Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-236-03

ICSA-21-168-03: **Advantech WebAccess/SCADA (Update A)**

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

ICSA-21-231-01: **AVEVA SuiteLink Server**

High level vulnerabilities: Heap-based Buffer Overflow, Null Pointer Dereference, Improper Handling of Exceptional Conditions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-231-01

ICSA-21-119-04: **Multiple RTOS (Update C)**

Critical level vulnerability: Integer Overflow or Wraparound.
https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04

ICSA-21-229-01: **ThroughTek Kalay P2P SDK**

Critical level vulnerability: Improper Access Control.
https://us-cert.cisa.gov/ics/advisories/icsa-21-229-01

ICSA-21-229-02: **Advantech WebAccess/NMS**

Medium level vulnerability: Improper Authentication.
https://us-cert.cisa.gov/ics/advisories/icsa-21-229-02

ICSA-21-229-03: **xArrow SCADA**

Medium level vulnerabilities: Cross-site Scripting, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-229-03

ICSA-21-224-01: **Cognex In-Sight OPC Server**

High level vulnerability: Deserialization of Untrusted Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-224-01

ICSA-21-224-02: Horner Automation Cscape

High level vulnerabilities: Out-of-bounds Write, Access of Uninitialized Pointer, Out-of-bounds Read.

https://us-cert.cisa.gov/ics/advisories/icsa-21-224-02

ICSA-21-182-02: Sensormatic Electronics C-CURE 9000 (Update A)

High level vulnerability: Improper Input Validation.

https://us-cert.cisa.gov/ics/advisories/icsa-21-182-02

ICSA-21-222-01: Siemens JT2Go and Teamcenter Visualization products

High level vulnerabilities: Use After Free, Out-of-bounds Write, Out-of-bounds Read, NULL Pointer Dereference.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-01

ICSA-21-222-02: Siemens Automation License Manager

Medium level vulnerability: Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-02

ICSA-21-222-03: Siemens JT2Go and Teamcenter Visualization

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

ICSA-21-222-04: Siemens SINEC NMS

High level vulnerability: OS Command Injection.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-04

ICSA-21-222-05: Siemens Industrial Products Intel CPUs

High level vulnerability: Missing Encryption of Sensitive Data.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-05

ICSA-21-222-06: Siemens Energy AGT and SGT Solutions

Critical level vulnerability: Out-of-bounds Write.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-06

ICSA-21-222-07: Siemens SIMATIC NET CP

High level vulnerabilities: Out-of-Bounds Read, Use After Free.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-07

ICSA-21-222-08: Siemens Solid Edge

High level vulnerabilities: Improper Restriction of XML External Entity Reference, Use After Free, Access of Uninitialized Pointer.

https://us-cert.cisa.gov/ics/advisories/icsa-21-222-08

ISCA-21-222-09: Siemens SIMATIC S7-1200

High level vulnerability: Improper Authentication.

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

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-21-194-07: Siemens Industrial Products LLDP (Update A)
Critical level vulnerabilities: Classic Buffer Overflow, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-07

ICSA-21-131-03: Siemens Linux-based Products (Update C)
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 B)
Critical 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-21-131-13: Siemens SINAMICS Medium Voltage Products Telnet (Update A)
High level vulnerability: Missing Authentication for Critical Function.
https://us-cert.cisa.gov/ics/advisories/icsa-21-131-13

ICSA-21-131-14: Siemens SCALANCE W1750D (Update A)
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-21-068-06: Siemens TCP/IP Stack Vulnerabilities–AMNESIA:33 in SENTRON PAC / 3VA Devices (Update B)
Medium level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-06

ICSA-20-315-04: Siemens SIMATIC S7-300 CPUs and SINUMERIK Controller (Update A)
Medium level vulnerability: Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-20-315-04

ICSA-20-070-01: Siemens and PKE SiNVR/SiVMS Video Server (Update B)
High level vulnerabilities: Cleartext Storage in a File or on Disk, Path Traversal, Improper Input Validation, Weak Cryptography for Passwords.
https://us-cert.cisa.gov/ics/advisories/icsa-20-070-01

ICSA-21-217-01: HCC Embedded InterNiche TCP/IP stack, NicheLite

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-21-217-02: FATEK Automation FvDesigner
High level vulnerabilities: Access of Uninitialized Pointer, Stack-based Buffer Overflow, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-217-02

ICSA-21-217-03: mySCADA myPRO
High level vulnerabilities: Improper Access Control, Unrestricted Upload of File with Dangerous Type, Path Traversal, Exposure of Information Through Directory Listing.
https://us-cert.cisa.gov/ics/advisories/icsa-21-217-03

ICSA-21-217-04: Advantech WebAccess SCADA
Critical level vulnerabilities: Cross-site Scripting (XSS), Relative Path Traversal, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-217-04

ICSMA-21-215-01: Swisslog Healthcare Translogic PTS
Critical level vulnerabilities: Use of Hard-coded Password, Execution with Unnecessary Privileges, Improper Authentication, Download of Code without Integrity Check, Out-of-Bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsma-21-215-01

ICSA-21-210-01: Hitachi ABB Power Grids eSOMS
High level vulnerability: Insufficiently Protected Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-210-01

ICSA-21-210-02: Wibu-Systems CodeMeter Runtime
Critical level vulnerability: Buffer Over-read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-210-02

ICSA-21-049-02: Mitsubishi Electric FA engineering software products (Update B)
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-21-208-01: KUKA KR C4
Critical level vulnerability: Use of Hard-Coded Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-208-01

ICSA-21-208-02: Mitsubishi Electric GOT2000 series and GT SoftGOT2000
Medium level vulnerability: Missing Synchronization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-208-02

ICSA-21-208-03: Geutebrück G-Cam E2 and G-Code

Critical level vulnerabilities: Missing Authentication for Critical Function, Command Injection, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-208-03

ICSA-21-208-04: LCDS LAquis SCADA

Critical level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-208-04

ICSA-21-208-05: Delta Electronics DIAScreen

High level vulnerabilities: Type Confusion, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-208-05

ICSA-21-194-02: Schneider Electric Modicon Controllers and Software (Update A)

Critical level vulnerabilities: Insufficiently Protected Credentials, Authentication Bypass by Spoofing, Deserialization of Untrusted Data, Missing Encryption of Sensitive Data.
https://us-cert.cisa.gov/ics/advisories/icsa-21-194-02

ICSA-21-182-03: Delta Electronics DOPSoft (Update A)

High level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-182-03

ICSA-21-180-05: AVEVA System Platform (Update A)

High level vulnerabilities: Missing Authentication for Critical Function, Uncaught Exception, Path Traversal, Origin Validation Error, Improper Verification of Cryptographic Signature.
https://us-cert.cisa.gov/ics/advisories/icsa-21-180-05

ICSA-21-112-02: Mitsubishi Electric GOT (Update A)

Medium level vulnerability: Improper Authentication.
https://us-cert.cisa.gov/ics/advisories/icsa-21-112-02

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

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

ICSA-21-201-01: Mitsubishi Electric MELSEC-F Series

High level vulnerability: NULL Pointer Dereference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-201-01

ICSMA-21-196-01: Ypsomed mylife

Medium level vulnerabilities: Insufficiently Protected Credentials, Not Using an Unpredictable IV with CBC Mode, Use of Hard-coded Credentials.
https://us-cert.cisa.gov/ics/advisories/icsma-21-196-01

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 August 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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