BLACK CELL
Információs értékei védelmében

2022. April, 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....2

ICS TRAININGS, EDUCATION....3

ICS CONFERENCES....7

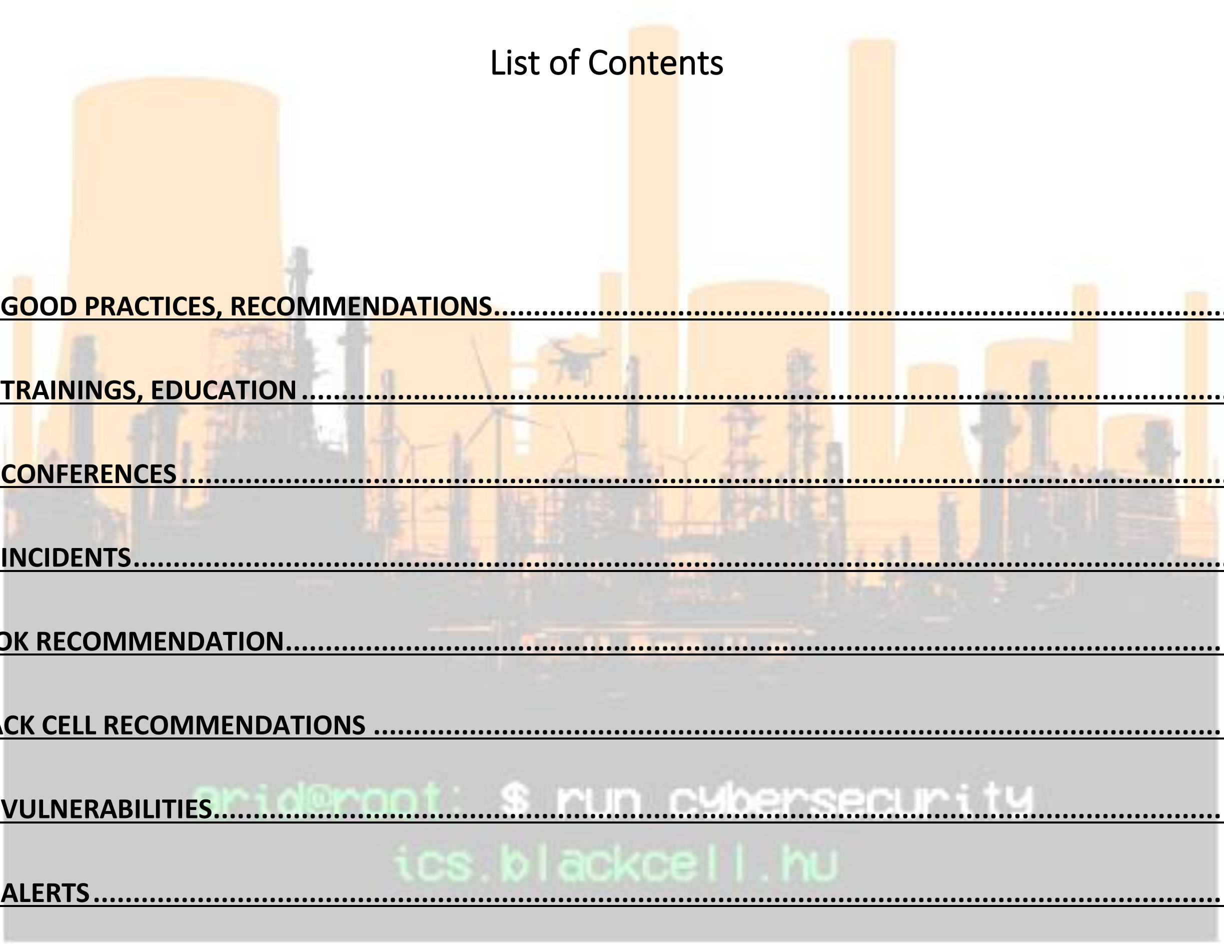
ICS INCIDENTS....9

BOOK RECOMMENDATION....10

BLACK CELL RECOMMENDATIONS....11

ICS VULNERABILITIES....12

ICS ALERTS....20



ICS good practices, recommendations

NIST SPECIAL PUBLICATION 1800-10

In March of 2022 the National Institute of Standards and Technology (NIST) released the NIST SPECIAL PUBLICATION 1800-10, Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector.

This new recommendation helps to the organizations, which operate IT and OT systems. The recommendation available and downloadable free for the interested organizations.

The publication helps to identify and mitigate the ICS integrity risks, strengthen, and harden the OT systems, and protect the data, which are very important to operate the ICSs securely.

The publications contain many common attack scenarios and provide many practical solutions to protect the IT and OT systems from the attackers. Insider threats are also a hot topic in the OT operation as well as the illegal remote accesses. The document provides examples how to mitigate these risks too.

Many collaborators helped to write the recommendations, and each organization is experienced in this issue. The collaborators are the following: Dispel, Dragos, Forescout, GreenTec, Microsoft, OSIsoft, Tenable, TDI, VMware.

Manufacturers are provided step-by-step instructions on how each vendor’s products can be installed and configured to address the described attack scenarios.

NIST is currently also working on another cybersecurity guide for manufacturers, one focusing on responding to and recovering from a cyberattack. That publication is currently a draft in the public comment period.

Source and more information available on the following link:

https://www.securityweek.com/nist-releases-ics-cybersecurity-guidance-manufacturers

NIST SPECIAL PUBLICATION 1800-10 available on this link:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-10.pdf

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in May 2022:

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:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

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 (201), (202)
- 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
  - 5-10. May 2022
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 5-10. May 2022
  - 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
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol NEW!!!
- Learn SCADA from Scratch - Design, Program and Interface NEW!!!

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/

The **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 or 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/

Bsigroup: Certified Lead SCADA Security Professional training course

This five-day training course will enable you to develop the expertise to plan, design and implement an effective programme to protect SCADA systems. You'll gain an understanding of common Industrial Control Systems (ICS) threats, vulnerabilities, and risks, and how they can be managed.

By attending this course you'll gain the knowledge and skills to advise on or manage risks related to SCADA environments and systems as a qualified professional. On successful completion of the PECB exam that takes place on the final day of this course, you'll gain Certified Lead SCADA Security Professional status.

Duration: 5 days, anytime at your office

More details can be found on the following website:

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

ICS/SCADA security training seminar

The courses are derived from 28 years of first-hand technology experience and industry best practices. The classes are customized to your team’s requirements and taught at your offices, classrooms and online live by world-class instructors with publications, patents, awards/honors, and a passion to share knowledge.

More details can be found on the following website:

https://www.enoinstitute.com/scada-ics-security-training-seminar/

ICS conferences

In May 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Cyber Security for Critical Assets Summit

CS4CA World will return virtually as a unique large-scale event to keep the critical asset community connected across the globe. As a worldwide 24-hour event, it will follow the sun by starting with speakers from the APAC region through to MENA, Europe, LatAm, finishing in North America. This unique format allows sponsors, speakers, and attendees to engage & connect with peers through a wide range of interactive content & networking formats much like a physical event.

As the global pandemic dramatically reshapes society into the new normal and fuels cyber threat workload, critical infrastructure organizations are busy reassessing their cyber risk while striving to maintain business continuity.

The summit offers dedicated sessions, allowing delegates to home in on their specialist areas of interest, as well as topics addressing the issues that bind both IT & OT professionals, with a focus on cyber resilience in a post-covid world. The agenda is curated by a group of industry-leading experts to be as relevant, cutting-edge, and as in-depth as possible over the 24-hour period.

Expect to feel inspired, educated and energised, with new ideas to take-away and try in your organisation as part of this innovative virtual conference.

Virtual event; May 5th, 2022

More details can be found on the following website:

https://world.cs4ca.com/

The Oil and Gas IoT Summit

IoT in the Oil and Gas industry is maturing. Moving from concept to strategy and now to daily applications which are making real, bottom-line improvements and delivering process efficiencies.

The Oil and Gas IoT Summit 2022 picks up the industry's transformation story post-pandemic. Focusing on case study evidence and lessons learned our speakers will share their personal experiences, challenges and REAL results. With one eye on the future, we'll also take a look at the key trends and developments that look set to shape the industry in the next 12 months and beyond.

Lisbon, Portugal; May 12nd -13rd, 2022

More details can be found on the following website:

https://apac.cs4ca.com/

Latin American SCADA Security Conference

Latin American SCADA Security Conference will bring together researchers with an interest in the safety of industrial control systems in light of their growing exposure in cyberspace. The topics of interest are broad, ranging from governance for industrial control systems to aspects of SCADA systems such as secure architectures, encryption, access control, and deep defense, among others.

Curitiba, Brazil; May 17th – 19th 2022

More details can be found on the following website:

https://10times.com/class-curitiba

ICS incidents

Ukrainian critical infrastructure as a target for cyber attacks

There are a lot of information and news about to the Ukrainian war and cyberwar. According to the Ukrainian governmental organizations, Russian hackers attacked the critical infrastructure, for example the power supply system.

In today’s critical situation in Ukraine, the availability of the communication systems is of utmost importance for both civilians and military purposes (sharing of information, location and fight against disinformation). One of the key targets for the Russian military is the satellite communication within and abroad in Ukraine and there are some news regarding the disruption of this key communication asset.

Western intelligence agencies are investigating the hacking of Viasat, which provides communications through a network of satellites. It appears to have been hit by a sophisticated cyber-attack that wiped devices on the day the invasion began.

Russian military forces also tried to jam Tesla’s SpaceX system within Ukraine, but they modified the firmware for the devices to make these jamming attempts unsuccessful. This is great example of cyber-physical resiliency and also a lesson to learn in the era of unpatchable IoT devices. (source: https://breakingdefense.com/2022/04/spacex-beating-russian-jamming-attack-was-eyewatering-dod-official/)

These constant threats from the cyber arm of the Russian military (like Cozy bear aka the APT29 group) made the Ukrainian government to recruit cyber security professionals from all hat colors in the world, to join their joint cyber-defense unit. (source: https://www.zdnet.com/article/ukraine-calls-for-underground-hackers-to-protect-critical-infrastructure-report/)

Ukraine also has some earlier experience regarding the attacks against critical infrastructure as their power grid was attacked in 2015, also by Russian actors.
(source:https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015))

What is interesting in this conflict is the lack of APT, 0-Day and mixed attacks against critical infrastructural targets, like the power grid or water and sewage systems. This is possibly due to the “Blitzkrieg”- like start of the war and the overly enthusiastic Russian military thinking on the start of this conflict, however we believe that there should be capabilities there, which could disrupt some infrastructural elements cyber-wise.

It’s very complicated to protect critical infrastructure in the cyberspace. Most of the vulnerabilities are published, and there are also zero-day vulnerabilities which are not. Many critical infrastructure operators recommend to monitor the news, which techniques are used in recent attacks and what are the indicators of compromise. If your organization is capable of such monitoring activities, the risks could be mitigated. If not, then monitoring is the first step of cyber-industrial resiliency.

The source and more information are available on the following link:
https://www.bbc.com/news/technology-60796079

Book recommendation

Industrial Network Security

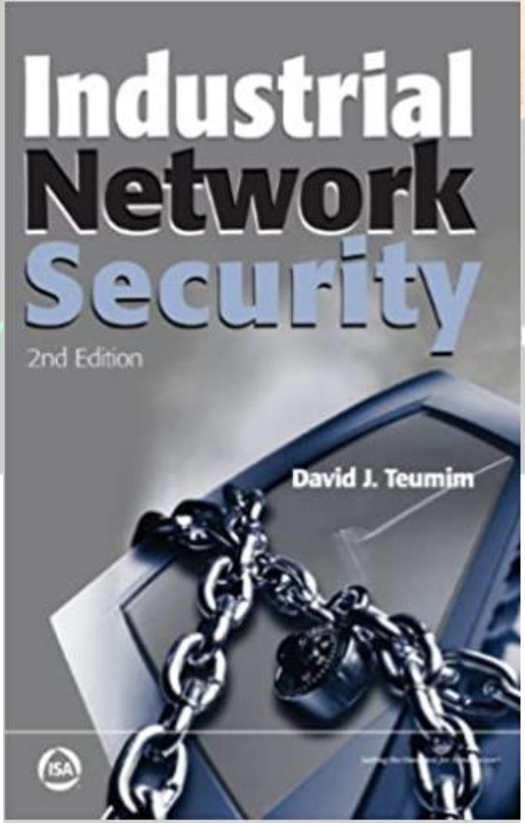
In the present days one only needs to read the newspaper headlines to appreciate the importance of industrial network security. Almost every day an article comes out describing the threat to the critical infrastructure, from spies in our electrical grid to the looming threat of cyber war. Whether we talk about process control systems that are running chemical plants and refineries, supervisory control and data acquisition (SCADA) systems for utilities, or factory automation systems for discrete manufacturing, the backbone of every nation’s critical infrastructure consists of these industrial networks and is dependent on their continued operation. This easy-to-read book introduces managers, engineers, technicians, and operators to methods for keeping our industrial networks secure amid rising threats from hackers, disgruntled employees, and even cyber terrorists.

Authors/Editors: David J. Teumim.

Year of issue: 2010 (Paperback) – Kindle edition 2016

The book is available at the following link:

https://www.amazon.com/Industrial-Network-Security-David-Teumim/dp/193600707X



Black Cell recommendations

Raising awareness in ICS cybersecurity

Everybody know the phrases, “the human is the weakest link” or “the problem exists between the keyboard and the chair”. There are many methods to raising the awareness, but many of these are very boring (for example awareness presentations, e-learning etc.).

What is a more interesting and exciting method is the “gamification”. There are a lot of possibility to raise awareness with games, for example information security escape room, card games and other interesting awareness solutions.

To get more familiar with gamification regarding IT/OT Security, we suggest to visit the Center for Development of Security Excellence, where you can find games regarding various topics of security, for free.

The following kind of games you can find:

- Industrial Security Concentrated Jeopardy games,
- Industrial Security Word Search,
- Security Awareness Crossword.

There are further games on the website, which are not closely connected to industrial security, but to IT Security and awareness in general. There is an Insider Threat Concentration Game, See something say something challenge and other very interesting games, which are suitable to raise the awareness to the gamified topics.

Try it, enjoy it, and if you have a chance, build it into the organizational awareness program.

More details and the games are available on the following link:

https://www.cdse.edu/Training/Security-Awareness-Games/

ICS vulnerabilities

In March 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-22-116-01: **Hitachi Energy System Data Manager**

High level vulnerabilities: Integer Overflow or Wraparound, Reachable Assertion, Type Confusion, Uncontrolled Recursion, Observable Discrepancy.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-116-01

ICSA-21-334-02: **Mitsubishi Electric MELSEC and MELIPC Series (Update B)**

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-334-02

ICSA-22-111-01: **Delta Electronics ASDA-Soft**

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-111-01

ICSA-22-111-02: **Johnson Controls Metasys SCT Pro**

Medium level vulnerability: Server-side Request Forgery.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-111-02

ICSA-22-111-03: **Hitachi Energy MicroSCADA Pro/X SYS600**

High level vulnerabilities: Observable Discrepancy, HTTP Request Smuggling, Classic Buffer Overflow, Improper Certificate Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer, Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-111-03

ICSA-22-109-01: **Interlogix Hills ComNav**

Medium level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Inadequate Encryption Strength.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-109-01

ICSA-22-109-02: **Automated Logic WebCTRL**

Medium level vulnerability: Open Redirect.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-109-02

ICSA-22-109-03: **FANUC ROBOGUIDE Simulation Platform**

Medium level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Improper Access Control, Path Traversal, Improper Restriction of XML External Entity Reference, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-109-03

ICSA-22-109-04: **Elcomplus SmartPPT SCADA**

Critical level vulnerabilities: Path Traversal, Unrestricted Upload of File with Dangerous Type, Improper Authorization, Cross-site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-109-04

ICSA-22-109-05: **Elcomplus SmartPPT SCADA Server**

Critical level vulnerabilities: Cross-site Scripting, Unauthorized Exposure to Sensitive Information, Unrestricted Upload of File with Dangerous Type, Path Traversal, Cross-site Request Forgery.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-109-05

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

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

ICSA-22-104-01: **Delta Electronics DMARS**

Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-01

ICSA-22-104-02: **Johnson Controls Metasys**

High level vulnerability: Incomplete Cleanup.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-02

ICSA-22-104-03: **Red Lion DA50N**

Critical level vulnerabilities: Insufficient Verification of Data Authenticity, Weak Password Requirements, Use of Unmaintained Third-Party Components, Insufficiently Protected Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-03

ICSA-22-104-04: **Siemens SCALANCE FragAttacks**

Medium level vulnerabilities: Improper Authentication, Injection, Improper Validation of Integrity Check, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-04

ICSA-22-104-05: **Siemens OpenSSL Vulnerabilities in Industrial Products**

Medium level vulnerability: NULL Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-05

ICSA-22-104-06: **Siemens PROFINET Stack Integrated on Interniche Stack**

Medium level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-06

ICSA-22-104-07: **Siemens Mendix**

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-07

ICSA-22-104-08: **Siemens SCALANCE W1700**

High level vulnerabilities: Race Condition, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-08

ICSA-22-104-09: Siemens SCALANCE X-300 Switches

Critical level vulnerabilities: Improper Input Validation, Use of Insufficiently Random Values, Stack-based Buffer Overflow, Cross-site Request Forgery, Improper Access Control, Basic XSS, Classic Buffer Overflow, Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-09

ICSA-22-104-10: Siemens SICAM A8000

Medium level vulnerability: Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-10

ICSA-22-104-11: Siemens SIMATIC Energy Manager

Critical level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Uncontrolled Search Path Element, Deserialization of Untrusted Data.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-11

ICSA-22-104-12: Siemens SIMATIC S7-400

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-12

ICSA-22-104-13: Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem

Critical level vulnerability: Use of Unmaintained Third-party Components.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-13

ICSA-22-104-14: Siemens SIMATIC STEP 7 (TIA Portal)

Medium level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-14

ICSA-22-104-15: Siemens Simcenter Femap

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

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-15

ICSA-22-104-16: Siemens TIA Administrator

High level vulnerability: Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-16

ICSA-22-104-17: Siemens Mendix

Low level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-17

ICSA-22-069-01: Siemens RUGGEDCOM Devices (Update A)

Medium level vulnerability: Missing Encryption of Sensitive Data.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-01

ICSA-22-069-08: Siemens Polarion ALM (Update A)

Medium level vulnerability: Cross-site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-08

ICSA-22-069-12: **Siemens RUGGEDCOM ROS (Update A)**

High level vulnerability: Using Components with Known Vulnerabilities.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-12

ICSA-22-069-13: **Siemens Mendix (Update A)**

Medium level vulnerability: Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-13

ICSA-22-041-02: **Siemens SIMATIC WinCC and PCS (Update A)**

Medium level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Insertion of Sensitive Information into Externally-Accessible File or Directory.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-02

ICSA-22-041-07: **Siemens Solid Edge, JT2Go, and Teamcenter Visualization (Update B)**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-07

ICSA-22-013-05: **Siemens COMOS Web (Update B)**

High level vulnerabilities: Basic XSS, Relative Path Traversal, SQL Injection, Cross-site Request Forgery.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-05

ICSA-21-315-03: **Siemens SIMATIC WinCC (Update C)**

Critical level vulnerabilities: Path Traversal, Insertion of Sensitive Information into Log File.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-03

ICSA-21-315-07: **Siemens Nucleus RTOS-based APOGEE and TALON Products (Update B)**

Critical level vulnerabilities: Type Confusion, Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Buffer Access with Incorrect Length Value, Integer Underflow, Improper Handling of Inconsistent Structural Elements.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-07

ICSA-21-222-05: **Siemens Industrial Products Intel CPUs (Update C)**

High level vulnerability: Missing Encryption of Sensitive Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-05

ICSA-21-194-03: **Siemens PROFINET Devices (Update D)**

High level vulnerability: Allocation of Resources Without Limits or Throttling.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-03

ICSA-21-194-12: **Siemens VxWorks-based Industrial Products (Update A)**

Critical level vulnerability: Heap-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-12

ICSA-21-159-13: Siemens SIMATIC RFID (Update A)
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-159-13

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

ICSA-20-105-06: Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update C)
High level vulnerability: Business Logic Errors.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-06

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update G)
High level vulnerability: Resource Exhaustion.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-07

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

ICSA-20-042-06: Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update G)
High level vulnerability: Incorrect Calculation of Buffer Size.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-042-06

ICSA-19-344-04: Siemens SIMATIC Products (Update C)
Low level vulnerability: Exposed Dangerous Method or Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-19-344-04

ICSA-19-099-03: Siemens Industrial Products with OPC UA (Update G)
High level vulnerability: Uncaught Exception.
https://www.cisa.gov/uscert/ics/advisories/ICSA-19-099-03

ICSA-17-243-01: Siemens OPC UA Protocol Stack Discovery Service (Update E)
High level vulnerability: Improper restriction of XML external entity reference.
https://www.cisa.gov/uscert/ics/advisories/ICSA-17-243-01-0

ICSA-16-327-01: Siemens SIMATIC CP 1543-1 (Update A)
Medium level vulnerabilities: Improper Input Validation, Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/ICSA-16-327-01

ICSA-22-102-01: Valmet DNA
High level vulnerability: Inadequate Encryption Strength.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-01

ICSA-22-102-02: Mitsubishi Electric MELSEC-Q Series C Controller Module
Critical level vulnerability: Heap-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-02

ICSA-22-102-03: **Inductive Automation Ignition**

Medium level vulnerability: Path Traversal.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-03

ICSA-22-102-04: **Mitsubishi Electric GT25-WLAN**

Medium level vulnerabilities: Improper Removal of Sensitive Information Before Storage or Transfer, Inadequate Encryption Strength, Missing Authentication for Critical Function, Injection, Improper Input Validation.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-04

ICSA-22-102-05: **Aethon TUG Home Base Server**

Critical level vulnerabilities: Missing Authorization, Channel Accessible by Non-endpoint, Cross-site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-05

ICSA-22-097-01: **Pepperl+Fuchs WirelessHART-Gateway**

Critical level vulnerabilities: Use of Hard-coded Credentials, Uncontrolled Resource Consumption, Reliance on Reverse DNS Resolution for a Security-critical Action, Path Traversal, Cross-site Scripting, Exposure of Sensitive Information to an Unauthorized Actor, Cleartext Storage of Sensitive Information in a Cookie, HTTP Request Smuggling, Sensitive Cookie Without 'HttpOnly' Flag, Cryptographic Issues.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-097-01

ICSA-22-097-02: **ABB SPIET800 and PNI800**

High level vulnerabilities: Incomplete Internal State Distinction, Improper Handling of Unexpected Data Type, Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-097-02

ICSA-21-278-01: **Mitsubishi Electric GOT and Tension Controller** (Update A)

High level vulnerabilities: Improper Handling of Exceptional Conditions, Improper Input Validation.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-278-01

ICSMA-22-095-01: **LifePoint Informatics Patient Portal**

Medium level vulnerability: Authentication Bypass Using Alternate Path or Channel.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-095-01

ICSA-22-095-01: **Rockwell Automation ISaGRAF**

High level vulnerability: Deserialization of Untrusted Data.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-095-01

ICSA-22-095-02: **Johnson Controls Metasys**

High level vulnerability: Server-side Request Forgery.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-095-02

ICSMA-21-187-01: Philips Vue PACS (Update B)

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Improper Authentication, Improper Initialization, Use of a Broken or Risky Cryptographic Algorithm, Protection Mechanism Failure, Use of a Key Past its Expiration Date, Insecure Default Initialization of Resource, Improper Handling of Unicode Encoding, Insufficiently Protected Credentials, Data Integrity Issues, Cross-site Scripting, Improper Neutralization, Use of Obsolete Function, Relative Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsma-21-187-01

ICSA-22-090-01: Schneider Electric SCADAPack Workbench

Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-01

ICSA-22-090-02: Hitachi Energy e-mesh EMS

High level vulnerabilities: Improper Restriction of Operations Within the Bounds of a Memory Buffer, Use After Free, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-02

ICSA-22-090-03: Fuji Electric Alpha5

High level vulnerabilities: Access of Uninitialized Pointer, Out-of-bound Read, Stack-based Buffer Overflow, Heap-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-03

ICSA-22-090-04: Mitsubishi Electric FA Products

High level vulnerabilities: Use of Password Hash Instead of Password for Authentication, Use of Weak Hash, Cleartext Storage of Sensitive Information, Authentication Bypass by Capture-replay.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-04

ICSA-22-090-05: Rockwell Automation Logix Controllers

Critical level vulnerability: Inclusion of Functionality from Untrusted Control Sphere.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-05

ICSA-22-090-06: General Electric Renewable Energy MDS Radios

Critical level vulnerabilities: Improper Input Validation, Hidden Functionality, Inadequate Encryption Strength, Uncontrolled Resource Consumption, Plaintext Storage of a Password, Download of Code Without Integrity Check.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-06

ICSA-22-090-07: Rockwell Automation Studio 5000 Logix Designer

High level vulnerability: Code Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-090-07

ICSA-22-067-01: PTC Axeda agent and Axeda Desktop Server (Update C)

Critical level vulnerabilities: Use of Hard-coded Credentials, Missing Authentication for Critical Function, Exposure of Sensitive Information to an Unauthorized Actor, Path Traversal, Improper Check or Handling of Exceptional Conditions.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01

ICSA-20-303-01: **Mitsubishi Electric MELSEC iQ-R, Q and L Series (Update C)**
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-303-01

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 April 2022, ICS-CERT published an alert

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

The cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations.

The following cybercrime groups pose a threat to critical infrastructure organizations: The CoomingProject, Killnet, MUMMY SPIDER, SALTY SPIDER, SCULLY SPIDER, SMOKEY SPIDER, WIZARD SPIDER, The Xaknet Team.

The cybercrime groups used the following malwares: Emotet, Trickbot, Conti Ransomware, and use DDoS to disrupt the critical infrastructures.

The alert mentioned the mitigation recommendations:

- Update software, including operating systems, applications, and firmware, on IT network assets.
- Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords.
- If you use RDP and/or other potentially risky services, secure and monitor them closely.
- Provide end-user awareness and training.
- Implement network segmentation to separate network segments based on role and functionality.

Recommended to preparing for cyber incidents in the following areas:

- Identity and Access Management,
- Protective Controls and Architecture,
- Vulnerability and Configuration Management,
- Responding to Cyber Incidents

Source and more information can be found at the following link:

https://www.cisa.gov/uscert/ncas/alerts/aa22-110a