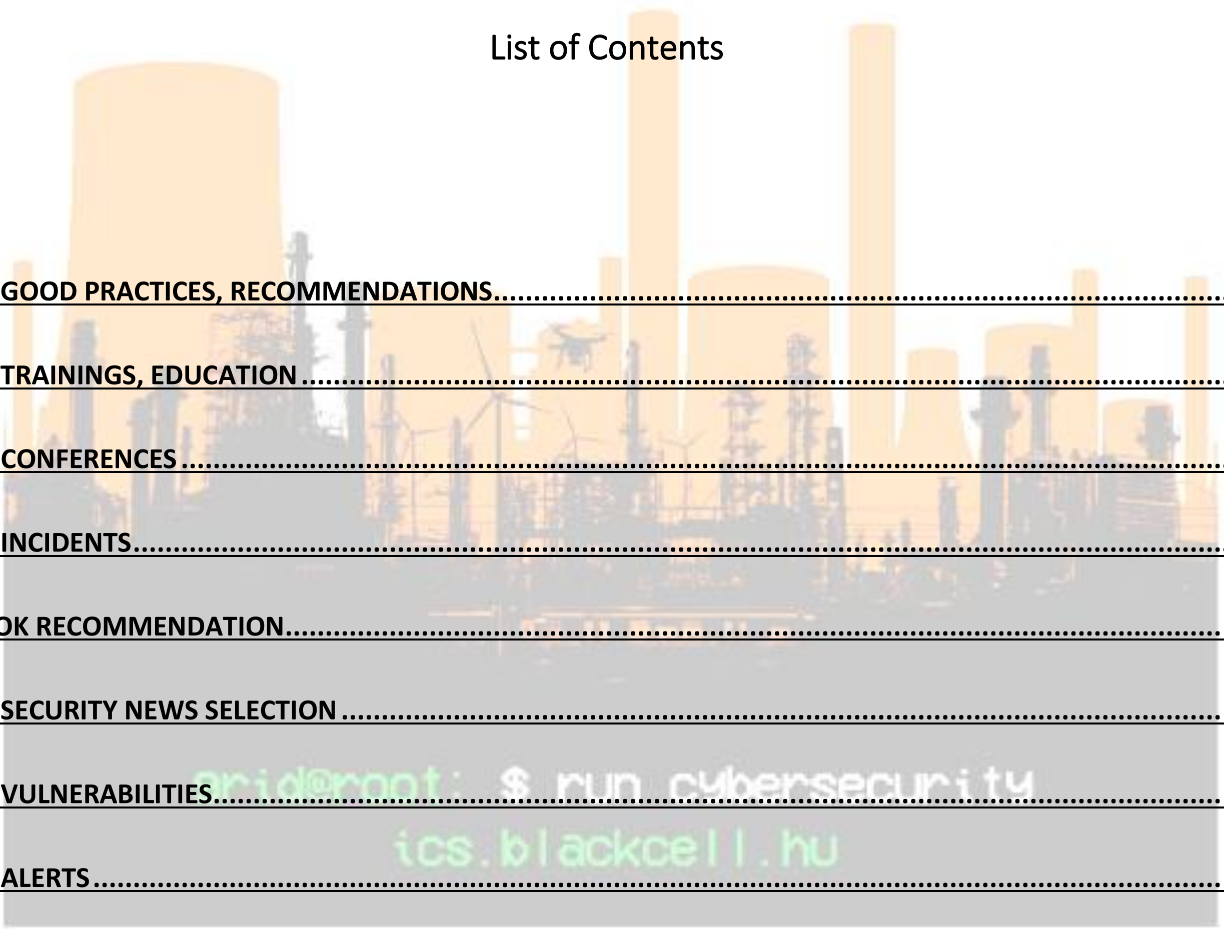
BLACK CELL
Információs értékei védelmében

2022 July, 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

Best Practices for Manufacturing OT Security

Amazon published a blogpost which presents a 5-point recommendation to separate OT (Operational Technology) systems used for managing operations of factories and industrial equipment.

The broad points to reach the goals are the following:

1. Secure all layers
2. Secure network connections to the cloud
3. Secure operational data
4. Enhance traceability and observability
5. Manage devices and gateways to shrink attack surface

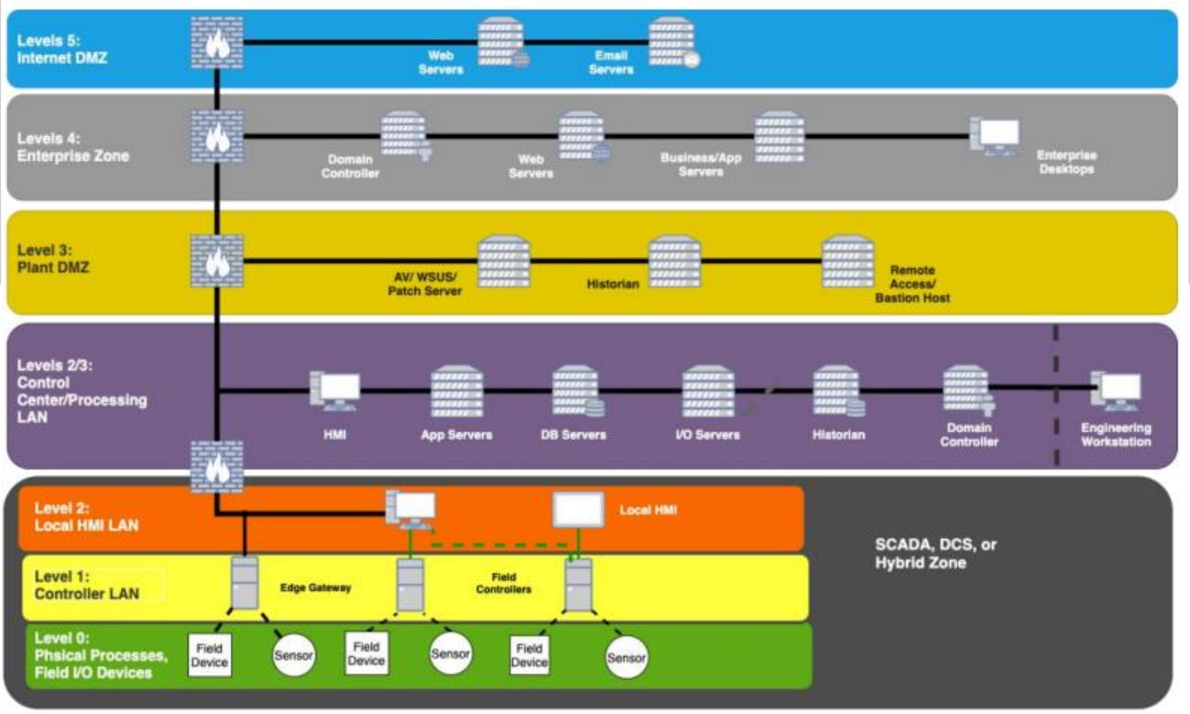
The blogpost is only a highlight from the Security Best Practices for Manufacturing OT Whitepaper, which is available on the following link:

https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf

The Whitepaper described the appropriate usage of the Purdue model, how to securely manage and access computing resources, and the necessity of continuously monitoring the network traffic and resources.

Source and more information available on the following link:

https://www.helpnetsecurity.com/2021/02/05/hardening-ge-cimplicity/



Source: https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf

ICS trainings, education

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

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
- ICS515: ICS Active Defense and Incident Response

More details can be found on the following websites:

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing
https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/#training-and-pricing

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
- Learn SCADA from Scratch - Design, Program and Interface

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.

Ethical Hacking for Industrial Control Systems

This exciting new and very advanced course supplies an environment to learn and apply offensive cyber operational (OCO) skills to a range of operational technology architectures. It introduces tactics, techniques, and procedures (TTP) to a range of real-world architectures, components, devices, and protocols that leverage both traditional software vulnerabilities and other more subtle, hard-to-find yet equally or more powerful human vulnerabilities that arise from typical system configuration and usage.

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

16. International Conference on Industrial Control Systems Security

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics and industry researchers. International Conference on Industrial Control Systems 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 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 Security.

Bangkok, Thailand; August 16th – 17th, 2022

More details can be found on the following website:

https://waset.org/industrial-control-systems-security-conference-in-august-2022-in-bangkok

9th Cyber & SCADA Security for Power and Utilities

In today's environment of digitization and integrated technologies, the utilities industry continues to face increased cybersecurity threats. More & more incidents in cyberspace are being reported annually by energy companies. Bolstering security and risk mitigation remain a serious challenge today and utility stakeholders can't avoid taking a commitment to cybersecurity to the front seat. One simply cannot afford to be out of the loop and underestimate vulnerabilities & risks that can await right around the corner.

Apart from advanced solutions & protection technologies available and constantly upgraded in the market, utilities also need to deploy the proper organization, to enhance awareness culture and ensure the security of its IT and OT systems is on the top of the agenda by their company leaders.

This virtual conference is a unique event gathering IT/OT security professionals specifically from Power & Utilities companies. It creates an excellent & interactive platform for our participants to share and brainstorm on common challenges, to exchange their ideas, and to network without leaving the desk.

Virtual event; August 19th; 2022

More details can be found on the following website:

https://www.prosperoevents.com/event/9th-cyber-scada-security-for-power-and-utilities-2022/

SCADA Technology Summit

SCADA Technology Summit is back in Dallas for 2022. The premiere SCADA & ICS conference in the world, SCADA Tech offers two days of educational sessions, networking and 1:1 meeting programs for attendees, speakers, and exhibitors. Attendees of the event will leave with the knowledge to improve their systems to enable them to better monitor/control equipment, optimize value, and harness valuable data to optimize processes.

- Learn the Latest Advancements in SCADA & ICS Technology
- Discover Advances in AI and Machine Learning in SCADA & ICS systems
- See How Others are Blending IoT/IIoT, SCADA and Networking Systems
- Bolster Security in Your SCADA and ICS Systems
- Enhance Your SCADA and ICS Systems with New Networking Technologies
- Stay Up-to-Date on the Latest SCADA Standard, Protocols and Regulations.

Dallas, Texas; August 24th – 25th, 2022

More details can be found on the following website:

https://www.scadatechsummit.com/

ICS incidents

Iranian state-owned Khuzestan Steel Company was hit by a cyber attack

Khuzestan Steel Company is one of the major producers of steel in the Middle East and among the top 10 in the world suffered a cyber-attack.

According to the company's information, the cyber-attack didn't cause damage to the production lines and impact on the supply chains, however the website was also shut down at the same time. Regardless of this information the organization's point of view is that the attack was unsuccessful.

The Iranian news channel Jamaran reported that the attack failed because at the time of the attack an electricity outage had interrupted the operations at the plant.

Neither the organization nor the Iranian government named the attackers.

In one of last year's most serious incidents, a cyber-attack on Iran's fuel distribution system paralyzed gas stations across the country, leading to dissatisfied drivers. In the last couple of years, Iranian infrastructure were hit by several cyber-attacks.

As it is customary today, we didn't know any technical or other detail of the attack.

The sources and more information are available on the following links:

https://securityaffairs.co/wordpress/132658/cyber-warfare-2/iran-khuzestan-steel-company-cyberattack.html

https://computerworld.hu/biztonsag/kibertamadas-miatt-leallt-az-irani-acelipari-vallalat-312946.html

Source: https://www.linkedin.com/authwall?trk=qf&original_referer=https://www.google.com/&sessionRedirect=https%3A%2F%2Fir.linkedin.com%2Fcompany%2Fkhouzestan-oxin-steel-company

Book recommendation

Pentesting Industrial Control Systems: An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes

The industrial cybersecurity domain has grown significantly in recent years. To completely secure critical infrastructure, red teams must be employed to continuously test and exploit the security integrity of an organization's people, processes, and products.

This is a unique pentesting book, which takes a different approach by helping you gain hands-on experience with equipment that you'll come across in the field. This will enable you to understand how industrial equipment interacts and operates within an operational environment.

You'll start by getting to grips with the basics of industrial processes, and then see how to create and break the process, along with gathering open-source intel to create a threat landscape for your potential customer. As you advance, you'll find out how to install and utilize offensive techniques used by professional hackers. Throughout the book, you'll explore industrial equipment, port and service discovery, pivoting, and much more, before finally launching attacks against systems in an industrial network.

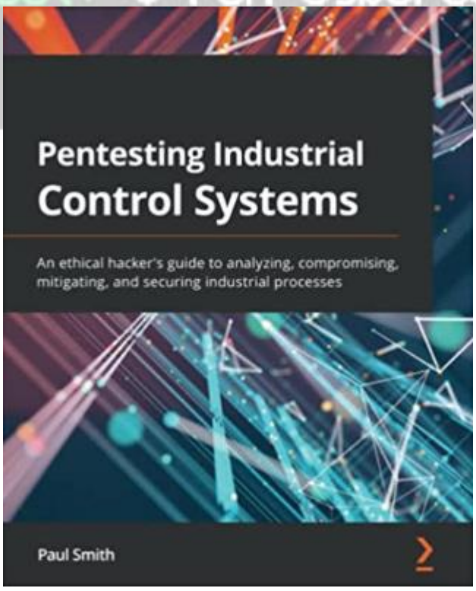
By the end of this penetration testing book, you'll not only understand how to analyze and navigate the intricacies of an industrial control system (ICS), but you'll develop essential offensive and defensive skills to proactively protect industrial networks from modern cyberattacks..

Authors/Editors: Paul Smith

Year of issue: 2021

The book is available at the following link:

https://www.amazon.com/Pentesting-Industrial-Control-Systems-compromising/dp/1800202385


Pentesting Industrial Control Systems
An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes
Paul Smith

ICS security news selection

House Passes ICS Cybersecurity Training Bill

The US House of Representatives has passed a new cybersecurity bill named the “Industrial Control Systems Cybersecurity Training Act.”

The bill was introduced in May by Rep. Eric Swalwell (D-CA), and it was approved by the House last week. Swalwell said the goal of the legislation is to help strengthen the US’s cybersecurity protections “in light of increased Russian cyber threats.”

Source and more information:
https://www.securityweek.com/house-passes-ics-cybersecurity-training-bill

Cyber-Physical Security: Benchmarking to Advance Your Journey

Over the last few years, the pandemic, rapid growth in several sectors and geographies, and the work from home paradigm shift have significantly accelerated the convergence of IT and operational technology (OT) networks and necessitated a consolidated strategy to address cyber risks across cyber-physical systems (CPS). Companies began to rise to the challenge and streamlined their IT and cybersecurity strategies to reflect this reality. This meant:

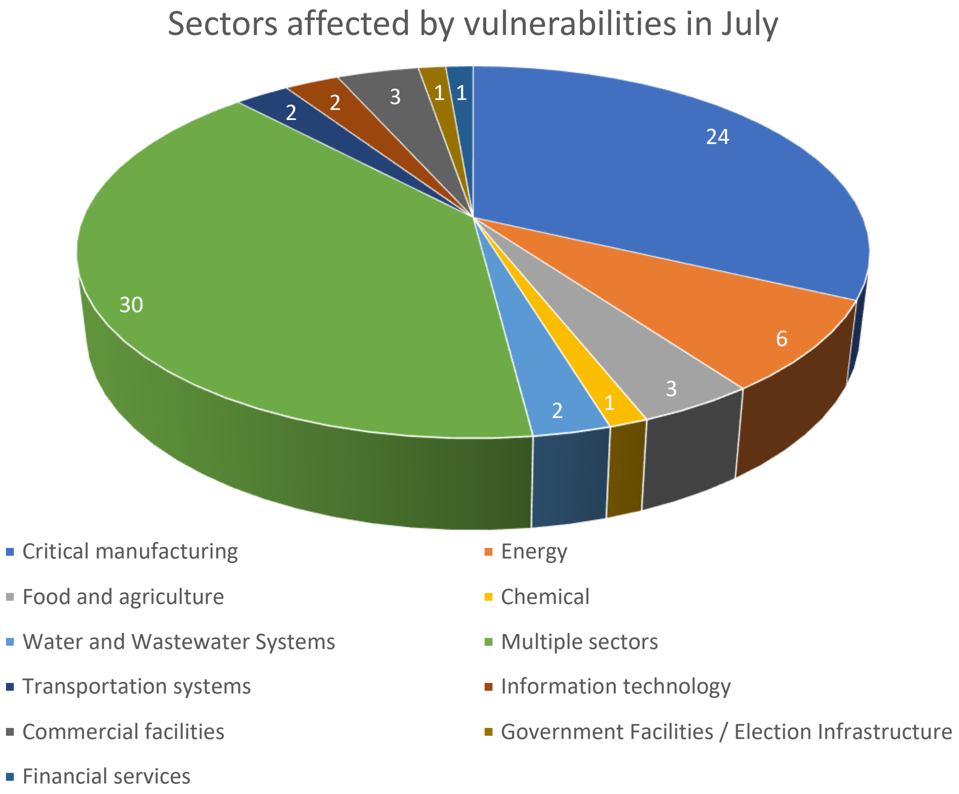
- Bringing OT and IT experts together to define a consolidated strategy
- Looking for efficiency and cost optimizations across the cybersecurity product stack that can address both fields
- Mapping their progress against an industry-defined and tested framework, to understand where they stand versus the competition and communicate risk and opportunities to the board

Cybersecurity, especially for CPS, evolved from being a cost factor, to an enabler for digital transformation, to a differentiating advantage for companies that truly excel at it.

Source and more information:
https://www.securityweek.com/cyber-physical-security-benchmarking-advance-your-journey

ICS vulnerabilities

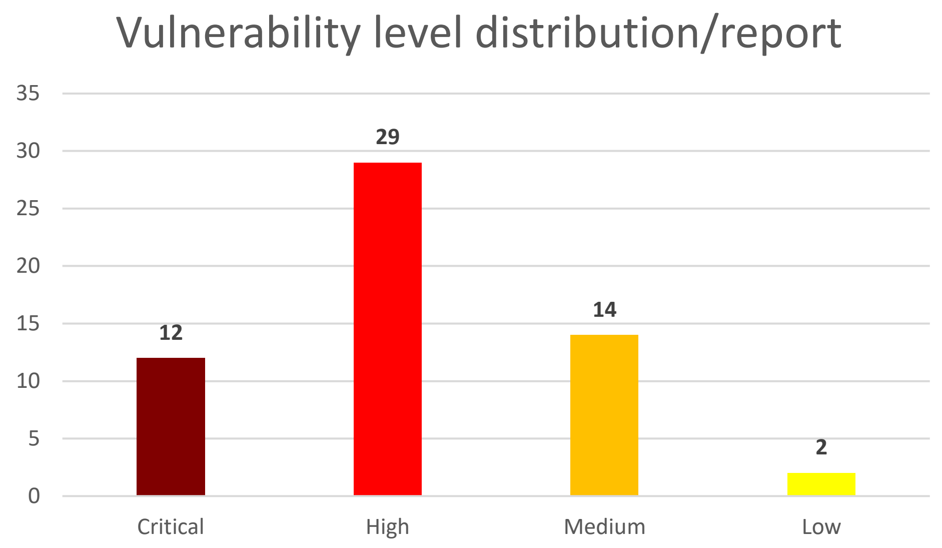
In July 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:



Average number of vulnerabilities per vulnerability report in July: **1,68**

The most common vulnerabilities in July:

Vulnerability	**CWE number**	**Piece**
Out-of-bounds Read	CWE-125	6
Missing Authentication for Critical Function	CWE-306	6
Improper Input Validation	CWE-20	5
Use of Hard-coded Credentials	CWE-798	5
Uncontrolled Resource Consumption	CWE-400	4
Heap-based Buffer Overflow	CWE-122	4
Improper Authentication	CWE-287	3



ICSA-22-209-01: **Rockwell Products Impacted by Chromium Type Confusion**
Low level vulnerability: Type Confusion.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-209-01

ICSA-21-350-05: **Mitsubishi Electric FA Engineering Software (Update B)**
Medium level vulnerabilities: Out-of-bounds Read, Integer Underflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-05

ICSA-20-212-02: **Mitsubishi Electric Factory Automation Engineering Software (Update C)**
High level vulnerability: Permission Issues.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-02

ICSA-22-207-01: **Inductive Automation Ignition**
High level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-01

ICSA-22-207-02: **Honeywell Safety Manager**
High level vulnerabilities: Insufficient Verification of Data Authenticity, Missing Authentication for Critical Function, Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-02

ICSA-22-207-03: **Honeywell Saia Burgess PG5 PCD**
High level vulnerabilities: Authentication Bypass, Use of a Broken or Risky Cryptographic Algorithm.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-03

ICSA-22-207-04: **MOXA NPort 5110**
High level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-207-04

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

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-22-202-01: ABB Drive Composer, Automation Builder, Mint Workbench

High level vulnerability: Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-01

ICSA-22-202-02: Johnson Controls Metasys ADS, ADX, OAS

Medium level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-02

ICSA-22-202-03: Rockwell Automation ISaGRAF Workbench

High level vulnerabilities: Deserialization of Untrusted Data, Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-03

ICSA-22-202-04: ICONICS Suite and Mitsubishi Electric MC Works64 Products

Critical level vulnerabilities: Path Traversal, Deserialization of Untrusted Data, Inclusion of Functionality from Untrusted Control Sphere, Out-of-Bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-04

ICSA-22-202-05: AutomationDirect Stride Field I/O

Critical level vulnerability: Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-202-05

ICSA-22-088-01: Rockwell Automation ISaGRAF (Update A)

Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-01

ICSA-22-200-01: MiCODUS MV720 GPS tracker

Critical level vulnerabilities: Use of Hard-coded Credentials, Improper Authentication, Cross-site Scripting, Authorization Bypass Through User-controlled Key.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-200-01

ICSA-22-193-01: Dahua ASI7213X-T1 (Update A)

High level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Authentication Bypass by Capture-replay, Generation of Error Message Containing Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-193-01

ICSA-22-195-01: Siemens SCALANCE X Switch Devices

Critical level vulnerabilities: Use of Insufficiently Random Values, Classic Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-01

ICSA-22-195-02: Siemens SICAM GridEdge

Medium level vulnerability: Exposure of Resource to Wrong Sphere.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-02

ICSA-22-195-03: **Siemens SIMATIC MV500 Devices**

High level vulnerabilities: Insufficient Session Expiration, Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-03

ICSA-22-195-04: **Siemens Simcenter Femap**

High level vulnerability: Out-of-bounds Write.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-04

ICSA-22-195-05: **Siemens RUGGEDCOM ROX**

High level vulnerability: Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-05

ICSA-22-195-06: **Siemens Mendix Excel Importer**

Medium level vulnerability: XML Entity Expansion.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-06

ICSA-22-195-07: **Siemens Datalogics File Parsing Vulnerability**

High level vulnerability: Heap-based buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-07

ICSA-22-195-08: **Siemens PADS Standard/Plus Viewer**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-08

ICSA-22-195-09: **Simcenter Femap and Parasolid**

High level vulnerability: Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-09

ICSA-22-195-10: **Siemens Mendix Applications**

Medium level vulnerability: Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-10

ICSA-22-195-11: **Open Design Alliance Drawings SDK**

High level vulnerability: Out-of-Bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-11

ICSA-22-195-12: **Siemens SRCS VPN Feature in SIMATIC CP Devices**

Critical level vulnerabilities: Heap-based Buffer Overflow, Command Injection, Code Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-12

ICSA-22-195-13: **Siemens Mendix**

Low level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-13

ICSA-22-195-14: **Siemens CPC80 Firmware of SICAM A8000**

High level vulnerability: Missing Release of Resource after Effective Lifetime.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-14

ICSA-22-195-15: **Siemens SIMATIC eaSie Core Package**

Critical level vulnerabilities: Improper Input Validation, Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-15

ICSA-22-195-16: **Siemens EN100 Ethernet Module**

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

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-16

ICSA-22-195-17: **Siemens Opcenter Quality**

Critical level vulnerability: Incorrect Implementation of Authentication Algorithm.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-17

ICSA-22-195-18: **Siemens RUGGEDCOM ROS**

High level vulnerability: Improper Control of Generation of Code.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-195-18

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

High level vulnerability: Missing Encryption of Sensitive Data.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-05

ICSA-22-041-01: **Siemens SIMATIC Industrial Products** (Update B)

High level vulnerabilities: Operation on a Resource after Expiration or Release, Missing Release of Memory after Effective Lifetime.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-01

ICSA-19-085-01: **Siemens SCALANCE X** (Update D)

Medium level vulnerability: Expected Behavior Violation.

https://www.cisa.gov/uscert/ics/advisories/ICSA-19-085-01

ICSA-22-104-16: **Siemens TIA Administrator** (Update A)

High level vulnerability: Uncontrolled Resource Consumption.

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

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

Critical level vulnerability: Heap-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-194-12

ICSA-22-104-06: **Siemens PROFINET Stack Integrated on Interniche Stack** (Update B)

Medium level vulnerability: Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-06

ICSA-22-132-08: Siemens Industrial Products with OPC UA (Update A)

Medium level vulnerability: Null Pointer Dereference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-08

ICSA-22-104-07: Siemens Mendix (Update B)

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-07

ICSA-22-167-14: Siemens OpenSSL Affected Industrial Products (Update A)

High level vulnerability: Infinite Loop.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-14

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

Critical level vulnerabilities: Path Traversal, Insertion of Sensitive Information into Log File.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-03

ICSA-22-132-05: Siemens Industrial PCs and CNC devices (Update A)

High level vulnerabilities: Improper Input Validation, Improper Authentication, Improper Isolation of Shared Resources on System-on-a-Chip, Improper Privilege Management.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-05

ICSA-22-132-12: Siemens Industrial Products (Update A)

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

https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-12

ICSA-22-193-01: Dahua ASI7213X-T1

High level vulnerabilities: Improper Input Validation, Unrestricted Upload of File with Dangerous Type, Authentication Bypass by Capture-replay, Generation of Error Message Containing Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-193-01

ICSA-22-055-03: Schneider Electric Easergy P5 and P3 (Update A)

High level vulnerabilities: Use of Hard-Coded Credentials, Classic Buffer Overflow, and Improper Input Validation.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-055-03

ICSA-22-188-01: Rockwell Automation MicroLogix

Medium level vulnerability: Improper Restriction of Rendered UI Layers or Frames.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-188-01

ICSA-22-188-02: Bently Nevada ADAPT 3701/4X Series and 60M100

Critical level vulnerabilities: Use of Hard-coded Credentials, Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-188-02

ICSA-21-280-04: **Mitsubishi Electric MELSEC iQ-R Series C Controller Module (Update B)**

Medium level vulnerability: Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-280-04

ICSA-22-181-01: **Exemys RME1**

Critical level vulnerability: Improper Authentication.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-01

ICSA-22-181-02: **Yokogawa Wide Area Communication Router**

Medium level vulnerability: Use of Insufficiently Random Values.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-02

ICSA-22-181-03: **Emerson DeltaV Distributed Control System**

High level vulnerabilities: Missing Authentication for Critical Function, Use of Hard-coded Credentials, Insufficient Verification of Data Authenticity, Use of a Broken or Risky Cryptographic Algorithm.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-03

ICSA-22-181-04: **Distributed Data Systems WebHMI**

Critical level vulnerabilities: Cross-site Scripting, OS Command Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-181-04

ICSA-21-350-05: **Mitsubishi Electric FA Engineering Software (Update A)**

Medium level vulnerabilities: Out-of-bounds Read, Integer Underflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-05

ICSA-15-258-02: **CODESYS Gateway Server (Update A)**

High level vulnerability: Heap Based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/ICSA-15-258-02

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In July 2022, ICS-CERT has published an alert:

North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

This sec feed shows only the IOCs:

Indicator Type	Value
Filename	maui.exe
	maui.log
	maui.key
	maui.evd
	aui.exe
MD5 Hash	4118d9adce7350c3eedeb056a3335346
	9b0e7c460a80f740d455a7521f0eada1
	fda3a19afa85912f6dc8452675245d6b
	2d02f5499d35a8dffb4c8bc0b7fec5c2
	c50b839f2fc3ce5a385b9ae1c05def3a
	a452a5f693036320b580d28ee55ae2a3
	a6e1efd70a077be032f052bb75544358
	802e7d6e80d7a60e17f9ffbd62fcbbeb
SHA256 Hash	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee48150616753fec4d6da16e99e
	45d8ac1ac692d6bb0fe776620371fca02b60cac8db23c4cc7ab5df262da42b78
	56925a1f7d853d814f80e98a1c4890b0a6a84c83a8eded34c585c98b2df6ab19
	830207029d83fd46a4a89cd623103ba2321b866428aa04360376e6a390063570
	458d258005f39d72ce47c111a7d17e8c52fe5fc7dd98575771640d9009385456
	99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21ef6fc2eb13521a930cea8bd9f
	3b9fe1713f638f85f20ea56fd09d20a96cd6d288732b04b073248b56cdaef878
	87bdb1de1dd6b0b75879d8b8aef80b562ec4fad365d7abbc629bcfc1d386afa6

More information is available on the following link:

https://www.cisa.gov/uscert/ncas/alerts/aa22-187a