2022 September, 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

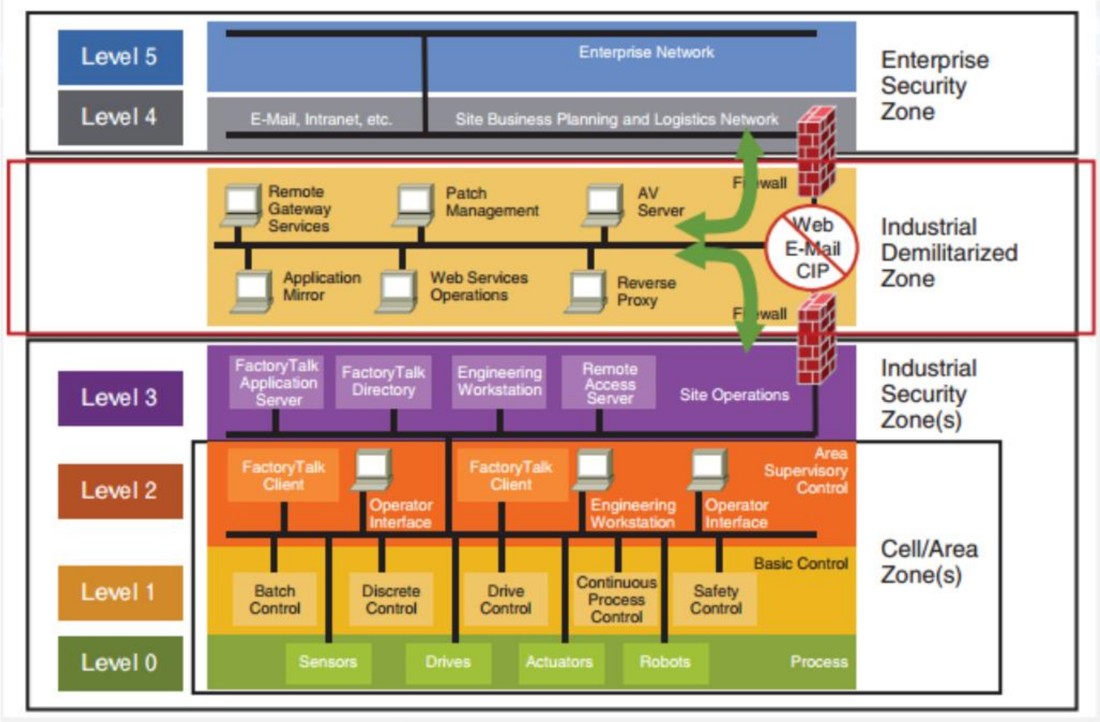
ICS good practices, recommendations

Purdue model

What Purdue model is?

The well-known Purdue Model of Computer Integrated Manufacturing has become an iconic standard in the automation world for its industrial control systems architecture guidance. The Purdue Model has helped provide industrial communication security through its separation of layers and definition of how machines and processes should function and interact.

It quickly became so well accepted that it influenced the ISA-95 standard that defines the interface between enterprise and control systems. And its prescribed data flows have also helped keep industrial networks deterministic by ensuring that control networks are not overwhelmed with non-production data.



If your organization is operating IT and OT, to implement the Purdue model is a key factor to ensure infrastructure-wide resilience.

Source and more information available on the following link:

https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in October 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/honours, and a passion to share knowledge.

More details can be found on the following website:

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

The Industrial Cyber Security Certification Course

This ICS Cybersecurity certification covers all aspects of Industrial Cyber security including a special advanced module on Understanding IEC 62443-2-4 that is very useful for not only automation system vendors and system integrators, but also to owners/operators to know what to expect from the vendor that supplies, installs, commissions and maintains the Industrial Control System.

When you complete the requirements of this course, you earn the title of CICP-Certified Industrial Cybersecurity Professional. (CICP)

More details can be found on the following website:

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

NEW in this security feed:

Secure IACS by ISA-IEC 62443 Standard

You'll learn on the Udemy course: Security of Industrial Automation and Control Systems (IACS), IOT Security, OT Security, ISA-IEC 62443

Initially, the ISA99 committee considered IT standards and practices for use in the IACS. However, it was soon found that this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS.

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to address the need to improve the cybersecurity of IACS.

This course includes:

- 1.5 hours on-demand video
- 1 article
- 1 downloadable resource
- Full lifetime access
- Access on mobile and TV
- Certificate of completion

More details can be found on the following website:

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

ICS conferences

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

IMI OT Community Days - in focus: attack detection 2022

Detecting cyber-attacks on IT and OT networks at an early stage and preventing their effects is a huge challenge that all operators have to face. For operators of critical infrastructure, the use of systems for attack detection is even mandatory in many countries.

The event will take place via live stream - you will have the opportunity to exchange ideas with the speakers and other participants in discussion rounds and networking breaks.

Online; October 11th 2022

More details can be found on the following website:

https://www.it-meets-industry.de/de/ot-cd/

IIoT World ICS Cybersecurity Day

One of a kind virtual conference series will bring together ICS cybersecurity subject matter experts from all over the world to share insights on IIoT technologies and ICS cybersecurity.

Some of the topics to be discussed are: Current Trends, Threats and Potential solutions; Applying a Zero Trust Mindset to Securing Industrial Control Systems; Designing cybersecurity for IoT; Leveraging Attack Surface Management Tactics to Improve ICS Security; Incentivizing ICS Cyber Protection through Insurance.

The content is targeted to CxOs, executives, as well as technology-oriented executives.

Online; October 12th 2022

More details can be found on the following website:

https://cybersecurity2022.iiotday.com/

Industrial Control Systems (ICS) Cyber Security Conference

SecurityWeek's ICS Cyber Security Conference is the conference where ICS users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyze their causes and cooperate on solutions. Since its first edition in 2002, the conference has attracted a continually rising interest as both the stakes of critical infrastructure protection and the distinctiveness of securing ICSs become increasingly apparent.

Atlanta, Georgia, USA; October 24th – 27th 2022

More details can be found on the following website:

https://www.icscybersecurityconference.com/

16. International Conference on Cyber Security of Industrial Control Systems

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 exceptional value for students, academics and industry researchers.

International Conference on Cyber Security of Industrial Control Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Security of Industrial Control Systems. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cyber Security of Industrial Control Systems.

Paris, France; October 27th – 28th 2022

More details can be found on the following website:

https://waset.org/cyber-security-of-industrial-control-systems-conference-in-october-2022-in-paris

ICS incidents

Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack

Cl0p ransomware group hacked the UK's largest water and wastewater company, which is responsible for 15 million people's water supply.

Thames Water said that the incident disrupted its corporate IT network and claimed that its ability to supply safe water has not been affected "thanks to the robust systems and controls over water supply and quality we have in place at all times".

Hackers gained access to all of the company's systems, including SCADA (supervisory control and data acquisition), the system what controlled the chemicals in the water.

Some news gives us screenshots, where you can see the HMI's that could potentially allow someone to tamper with industrial control systems (ICS).

The water system's alerting is well organized, and the company explained that if the hackers changed the composition of the chemicals, the PLC alerted the competent persons, who would took measures.

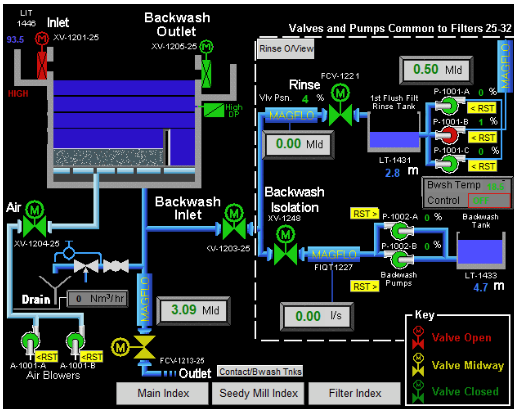
The cybercriminals claim to have stolen more than 5 Tb of information after spending months in the company's networks.

It is not uncommon to target OT systems because of the vulnerabilities of legacy devices.

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

https://www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack

https://www.itpro.co.uk/security/ransomware/368808/uk-water-supplier-confirms-hack-by-cl0p-ransomware-gang



Source: https://www.securityweek.com/ransomware-group-claims-access-scada-confusing-uk-water-company-hack

Book recommendation

Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems

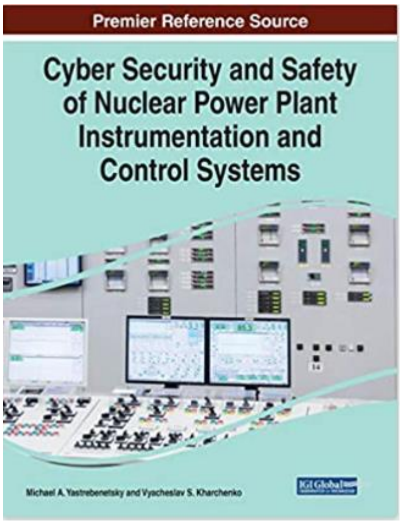
Safety and security are crucial to the operations of nuclear power plants, but cyber threats to these facilities are increasing significantly. Instrumentation and control systems, which play a vital role in the prevention of these incidents, have seen major design modifications with the implementation of digital technologies. Advanced computing systems are assisting in the protection and safety of nuclear power plants; however, significant research on these computational methods is deficient. Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems is a pivotal reference source that provides vital research on the digital developments of instrumentation and control systems for assuring the safety and security of nuclear power plants. While highlighting topics such as accident monitoring systems, classification measures, and UAV fleets, this publication explores individual cases of security breaches as well as future methods of practice. This book is ideally designed for engineers, industry specialists, researchers, policymakers, scientists, academicians, practitioners, and students involved in the development and operation of instrumentation and control systems for nuclear power plants, chemical and petrochemical industries, transport, and medical equipment.

Authors/Editors: Michael A. Yastrebenetsky (Editor), Vyacheslav S. Kharchenko (Editor)

Year of issue: 2020

The book is available at the following link:

https://www.amazon.com/Security-Nuclear-Instrumentation-Control-Systems/dp/1799832783


Premier Reference Source
Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems
Michael A. Yastrebenetsky and Vyacheslav S. Kharchenko
IGI Global

ICS security news selection

Analysis of Ragnar Locker Ransomware that has been targeting the energy sector

The Ragnar group, operating Ragnar Locker ransomware, has been active since 2019 targeting critical industries and employing double extortion. In March 2022, the FBI warned that at least 52 entities across ten critical industry sectors have been affected. In August 2022, the group attacked Greek gas supplier Desfa, and subsequently leaked sensitive data it claimed to have stolen.

Researchers at Cybereason have analyzed the encryption process of Ragnar Locker.

On execution, Ragnar Locker does a location check. If the location is any country in the Commonwealth of Independent States (CIS), execution is terminated. …

Source and more information:

https://www.securityweek.com/deep-dive-ragnar-locker-ransomware-targeting-critical-industries

There is no secure critical infrastructure without identity-based access

Organizational security strategy has long been defined by an internal perimeter enclosing all a company's information in a single secure location. Designed to keep external threats out through firewalls and other intrusion prevention systems, this security model permits trusted insiders virtually unrestricted access to corporate IT assets and resources. Practically speaking, this means any user who has access to the network could also access proprietary and sensitive information, regardless of their job title or requirements.

As companies continue to struggle with differentiating between authorized users and attackers, many are turning to identity-based solutions to better secure their systems while maintaining business continuity and employee productivity. In fact, Gartner forecasts that by 2024, 30% of large enterprises will implement new identity-proofing tools to address common weaknesses in workforce identity processes and networks.

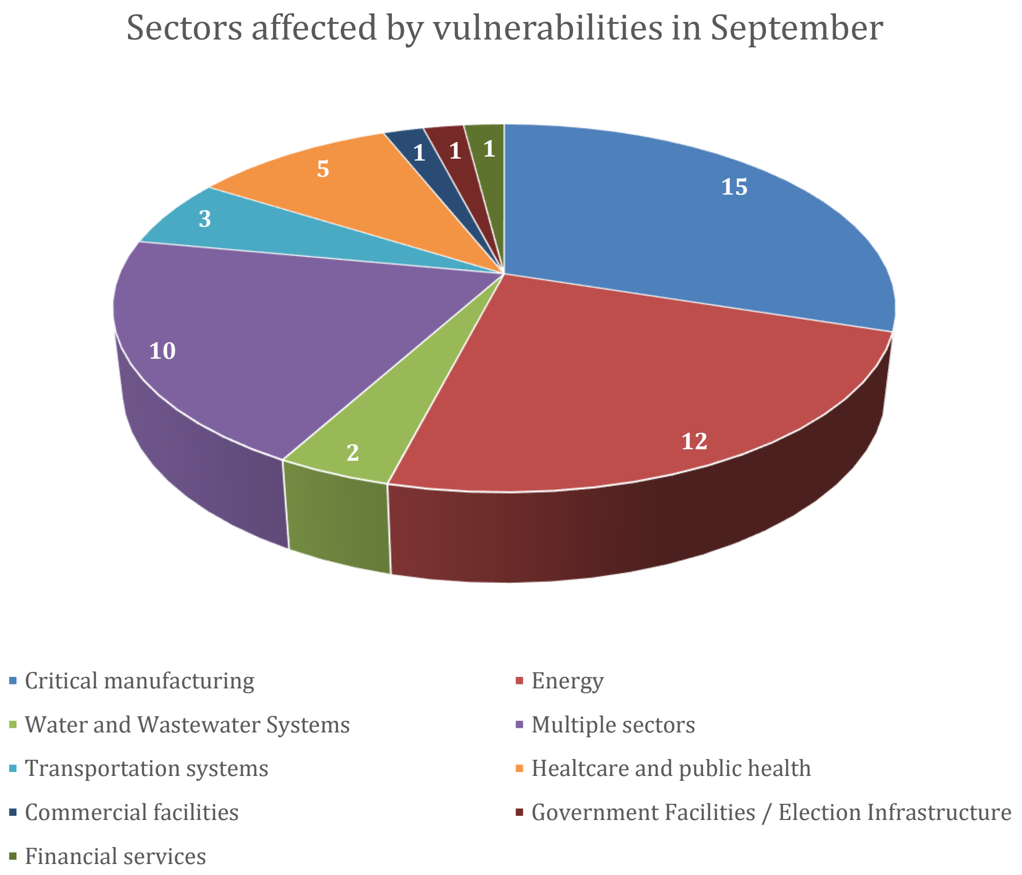
Unfortunately, critical infrastructure organizations are lagging far behind when it comes to adopting identity-based security and modernizing their systems, which often include both operational technology (OT) and information technology (IT) components. …

Source and more information:

https://www.helpnetsecurity.com/2022/09/07/critical-infrastructure-identity-based-access/

ICS vulnerabilities

In September 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:

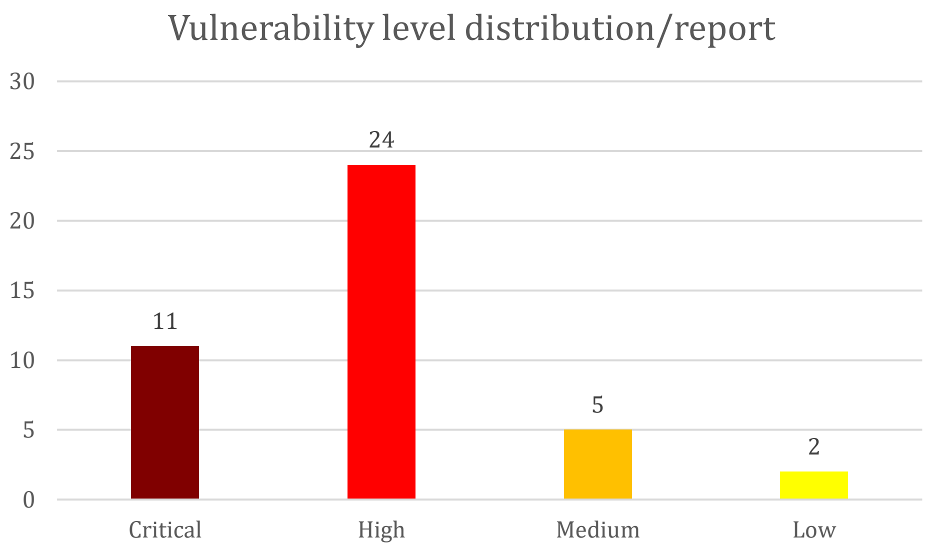


Average number of vulnerabilities per vulnerability report in September: **2,14**

The most common vulnerabilities in September:

Vulnerability	CWE number	Piece
Improper Access Control	CWE-284	6
Out-of-bounds Read	CWE-125	5
Stack-based Buffer Overflow	CWE-121	5

Improper Input Validation	CWE-20	4
Uncontrolled Resource Consumption	CWE-400	4
Improper Authentication	CWE-287	3
Heap-based Buffer Overflow	CWE-122	3
Out-of-bounds Write	CWE-787	3
Use of Hard-coded Credentials	CWE-798	3
Missing Encryption of Sensitive Data	CWE-311	3



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

High level vulnerability: Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-182-03

ICSA-22-272-02: **Hitachi Energy MicroSCADA Pro X SYS600**

High level vulnerabilities: NULL Pointer Dereference, Infinite Loop.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-272-02

ICSA-22-272-01: **Hitachi Energy MicroSCADA Pro X SYS600**

High level vulnerabilities: Improper Input Validation, Improper Privilege Management, Improper Access Control, Improper Handling of Unexpected Data Type.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-272-01

ICSA-22-270-01: **Hitachi Energy AFS660/AFS665**

Critical level vulnerability: Improper Input Validation.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-270-01

ICSA-22-270-02: **Hitachi Energy APM Edge**

High level vulnerabilities: Out-of-Bounds Write and Improper Authentication.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-270-02

ICSA-22-270-03: **Rockwell Automation ThinManager ThinServer**

High level vulnerability: Heap-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-270-03

ICSA-22-265-01: **Measuresoft ScadaPro Server**

High level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-265-01

ICSA-20-212-02: **Mitsubishi Electric Factory Automation Engineering Software (Update D)**

High level vulnerability: Permission Issues.

https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-02

ICSA-20-245-01: **Mitsubishi Electric Multiple Products (Update E)**

High level vulnerability: Predictable Exact Value from Previous Values.

https://www.cisa.gov/uscert/ics/advisories/icsa-20-245-01

ICSA-22-263-01: **Hitachi Energy PROMOD IV**

Critical level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-01

ICSA-22-263-02: **Hitachi Energy AFF660/665 Series**

Critical level vulnerability: Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-02

ICSMA-22-263-01: **Medtronic NGP 600 Series Insulin Pumps**

Low level vulnerability: Protection Mechanism Failure.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-263-01

ICSA-22-263-03: **Dataprobe iBoot-PDU**

Critical level vulnerabilities: OS Command Injection, Path Traversal, Exposure of Sensitive Information to an Unauthorized Actor, Improper Access Control, Improper Authorization, Incorrect Authorization, SSRF.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03

ICSA-22-263-04: **Host Engineering Communications Module**

Medium level vulnerability: Stack-based Buffer overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-04

ICSA-22-167-03: **AutomationDirect DirectLOGIC with Ethernet (Update A)**

High level vulnerabilities: Uncontrolled Resource Consumption, Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-03

ICSA-22-167-02: **AutomationDirect DirectLOGIC with Serial Communication (Update A)**

High level vulnerability: Cleartext Transmission of Sensitive Information.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-167-02

ICSA-22-200-01: **MiCODUS MV720 GPS tracker (Update A)**

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-22-258-01: **Siemens Mobility CoreShield OWG Software**

High level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-258-01

ICSA-22-258-02: **Siemens Simcenter Femap and Parasolid**

High level vulnerability: Multiple File Parsing Vulnerabilities (Out-of-bounds Read, Access of Uninitialized Pointer, Out-of-bounds Write).

https://www.cisa.gov/uscert/ics/advisories/icsa-22-258-02

ICSA-22-258-03: **Siemens RUGGEDCOM ROS**

Medium level vulnerability: Uncontrolled Resource Consumption.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-258-03

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

High level vulnerability: Missing Encryption of Sensitive Data.

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

ICSA-22-258-04: **Siemens Mendix SAML Module**

High level vulnerability: Authentication Bypass by Capture-replay.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-258-04

ICSA-22-258-05: **Siemens SINEC INS**

High level vulnerabilities: Improper Input Validation, Integer Overflow or Wraparound, Uncontrolled Resource Consumption, Command Injection, Inadequate Encryption Strength, Missing Encryption of Sensitive Data, Improper Restriction of Operations Within the Bounds of a Memory Buffer, Exposure of Private Personal Information to an Unauthorized Actor, Open Redirect, Improper Resource Shutdown or Release, Server-Side Request Forgery (SSRF).

https://www.cisa.gov/uscert/ics/advisories/icsa-22-258-05

ICSA-19-344-03: **Siemens RUGGEDCOM ROS (Update A)**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Resource Management Errors.

https://www.cisa.gov/uscert/ics/advisories/icsa-19-344-03

ICSA-22-195-09: **Simcenter Femap and Parasolid (Update B)**

High level vulnerability: Out-of-bounds Read.

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

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

High level vulnerability: Infinite Loop.

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

ICSA-22-223-07: **Siemens SCALANCE (Update A)**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Allocation of Resources Without Limits or Throttling, Basic Cross Site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-223-07

ICSA-22-256-03: **Delta Industrial Automation DIAEnergie**

Critical level vulnerability: Use of Hard-coded Credentials.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-03

ICSA-22-256-04: **Kingspan TMS300 CS**

Critical level vulnerability: Improper Authentication.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-04

ICSA-22-256-02: **Honeywell SoftMaster**

High level vulnerabilities: Uncontrolled Search Path Element, Incorrect Permission Assignment for Critical Resource.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-02

ICSA-22-256-01: **Hitachi Energy TXpert Hub CoreTec 4 Sudo Vulnerability**

High level vulnerability: Off-by-one Error.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-256-01

ICSMA-22-251-01: **Baxter Sigma Spectrum Infusion Pump**

Medium level vulnerabilities: Missing Encryption of Sensitive Data, Use of Externally Controlled Format String, Missing Authentication for Critical Function.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-251-01

ICSA-22-251-01: **MZ Automation libIEC61850**

Critical level vulnerabilities: Buffer Overflow, Access of Resource Using Incompatible Type, NULL Pointer Dereference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-251-01

ICSMA-21-152-01: **Hillrom Medical Device Management (Update B)**

Medium level vulnerabilities: Out-of-Bounds Write, Out-of-Bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsma-21-152-01

ICSA-22-242-10: **PTC Kepware KEPServerEX (Update A)**

Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-10

ICSA-22-249-01: **Triangle Microworks Libraries**

High level vulnerability: Access of Uninitialized Pointer.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-01

ICSA-22-249-02: **AVEVA Edge 2020 R2 SP1 and all prior versions**

High level vulnerabilities: Insufficient UI Warning of Dangerous Operations, Uncontrolled Search Path Element, Deserialization of Untrusted Data, Improper Restriction of XML External Entity Reference.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-02

ICSA-22-249-03: **Cognex 3D-A1000 Dimensioning System**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Output Neutralization for Logs, Client-side Enforcement of Server-side Security.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-03

ICSA-22-249-04: **Hitachi Energy TXpert Hub CoreTec 4**

Medium level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Improper Input Validation, Download of Code Without Integrity Check.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-249-04

ICSA-21-252-02: **Delta Electronics DOPSoft 2 (Update A)**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-Bounds Write, Heap-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-21-252-02

ICSMA-22-244-01: **Contec Health CMS8000**

High level vulnerabilities: Improper Access Control, Uncontrolled Resource Consumption, Use of Hard-Coded Credentials, Active Debug Code.

https://www.cisa.gov/uscert/ics/advisories/icsma-22-244-01

ICSA-22-244-01: **Delta Electronics DOPSoft**

Low level vulnerability: Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-244-01

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 September 2022, ICS-CERT has published an alert:

Control System Defense: Know the Opponent

Operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors. These cyber actors, including advanced persistent threat (APT) groups, target OT/ICS assets to achieve political gains, economic advantages, or destructive effects. Because OT/ICS systems manage physical operational processes, cyber actors' operations could result in physical consequences, including loss of life, property damage, and disruption of National Critical Functions.

OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks.

Traditional approaches to securing OT/ICS do not adequately address current threats to those systems. However, owners and operators who understand cyber actors' tactics, techniques, and procedures (TTPs) can use that knowledge when prioritizing hardening actions for OT/ICS.

This joint Cybersecurity Advisory, which builds on previous NSA and CISA guidance to stop malicious ICS activity and reduce OT exposure, describes TTPs that malicious actors use to compromise OT/ICS assets. It also recommends mitigations that owners and operators can use to defend their systems. NSA and CISA encourage OT/ICS owners and operators to apply the recommendations in this CSA.

The following can be found in detail on the website:

- Technical Details
- Malicious actors' game plan for control system intrusions
- Establish intended effect and select a target
- Collect intelligence about the target system
- Develop techniques and tools
- Gain initial access to the system
- Execute techniques and tools to create the intended effects
- Mitigations
- Limit exposure of system information
- Identify and secure remote access points

- Restrict tools and scripts
- Conduct regular security audits
- Implement a dynamic network environment
- Conclusion
- Disclaimer of endorsement
- Purpose
- Contact Information
- References

Source and more information can be found on the website:

https://www.cisa.gov/uscert/ncas/alerts/aa22-265a

.