# 2022 October, Industrial Control Systems security feed

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

## List of Contents

# ICS good practices, recommendations

**Mitigate OT security threats with these best practices**

The security community is continuously changing, growing, and learning from each other to position the world better against cyber threats. In the latest "Voice of the Community" blog series post, Microsoft Product Marketing Manager Natalia Godyla talks with Chris Sistrunk, Technical Manager in Mandiant's ICS/OT Consulting practice and former engineer at Entergy, where he was a subject matter expert on transmission and distribution of supervisory control and data acquisition (SCADA) systems. In this blog, Chris shares best practices to help mitigate the security threats to operational technology (OT) environments.

The conversation is very exciting and the information what's shared by Chris is very useful. It contains a multitude of interesting subjects, like which tools can help to monitor and govern the OT environment, what are the best practices for securing remote access to the OT network, what percentage of organizations are continuously monitoring their OT networks, or should companies unify IT and OT security in the security operations center (SOC).

We strongly recommend reading the conversation, as the information shared within will be very useful if you want to establish a well-organized and resilient OT security.

Source and more information available on the following link:

https://www.microsoft.com/security/blog/2021/05/18/mitigate-ot-security-threats-with-these-best-practices/

## ICS trainings, education

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

**Secure IACS by ISA-IEC 62443 Standard**

The subjects of this 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 November 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

### Dragos Industrial Security Conference 2022

At DISC (Dragos Industrial Security Conference) 2022, you'll hear ICS research on threats, malware, incidents, and vulnerabilities conducted by its intelligence and threat operations teams. The program is technical, research-oriented, and contains actionable advice based on lessons from the field.

Due to the sensitivity of information shared, the exclusive content presented as a day-long series of presentations will not be publicly available afterward.

Hanover, MD, USA; 5th November 2022

More details can be found on the following website:

https://www.dragos.com/disc/

### Industrial Security Conference in Copenhagen

The energy sector is one of the main targets of critical infrastructure in terms of cyber-attacks and hacking, but it is not the only one. Transportation, public sector services, telecommunications and critical manufacturing industries are also targets. It is especially dangerous and costly because it disrupts necessities such as water, heat, healthcare, and food supply. Cybercrime is growing, new vulnerabilities are discovered every day, cybercriminals are increasingly collaborating, and new types of malware are staying undetected. The threat landscape is ever changing and so are the tools necessary to keep networks, IT/OT systems, and people protected from cyber-attacks.

Presentations from leading experts around the world, rewarding keynotes, knowledge sharing and networking with international peers in the industry.

Copenhagen, Denmark; 14-16th November 2022

More details can be found on the following website:

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

### National SCADA Conference

The National SCADA Conference now in its 20th year is the largest and longest running event for Australia and New Zealand's SCADA sectors. The conference and associated networking functions brings the industry together to network, learn, share stories and experiences.

This year's programme will facilitate insightful debates on the most critical strategies, technical and business issues, for successful SCADA systems. It will equip you and your team with up-to-date practical advice to make informed and profitable decisions.

Melbourne, Australia, 24-25th November 2022

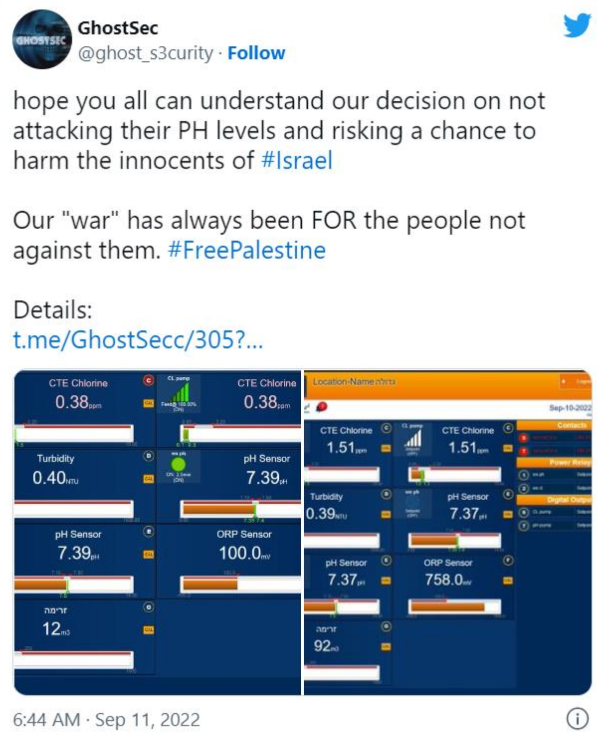
More details can be found on the following website:

https://scada-conference.com/

## ICS incidents

### 55 Berghof programmable logic controllers (PLCs) hacked

Pro-Palestinian Hacking Group GhostSec published that they hacked 55 Berghof programmable logic controllers (PLCs) used by Israeli organizations as part of a Free Palestine campaign. The incident appeared in the social media platforms:



GhostSec
@ghost_s3curity · Follow

hope you all can understand our decision on not attacking their PH levels and risking a chance to harm the innocents of #Israel

Our "war" has always been FOR the people not against them. #FreePalestine

Details:
t.me/GhostSecc/305?...

6:44 AM · Sep 11, 2022

The hacking group also published a video, where they demonstrated the successful PLC login with admin access, and blocked the PLC.

Cybersecurity experts pointed out, that the default and common credentials used for logging in to the PLCs admin panels with full permission.

Cybersecurity experts explained that the attack didn't harm the OT systems, the aim of the attackers was to draw attention to the hacktivist group and its activities.

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

https://securityaffairs.co/wordpress/135656/hacktivism/ghostsec-hacked-berghof-plcs-israel.html

https://industrialcyber.co/critical-infrastructure/ghostsec-hacktivist-group-compromise-55-berghof-plcs-across-israel-otorio-discloses/

## Book recommendation

**Operational Technology Security A Complete Guide**

This Operational Technology Security Guide is unlike the books you're used to. If you're looking for a textbook, this might not be for you. This book and its included digital components are for who understands the importance of asking great questions. This gives you the questions to uncover the Operational Technology Security challenges you're facing and generate better solutions to solve those problems.

Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role… In EVERY group, company, organization and department.

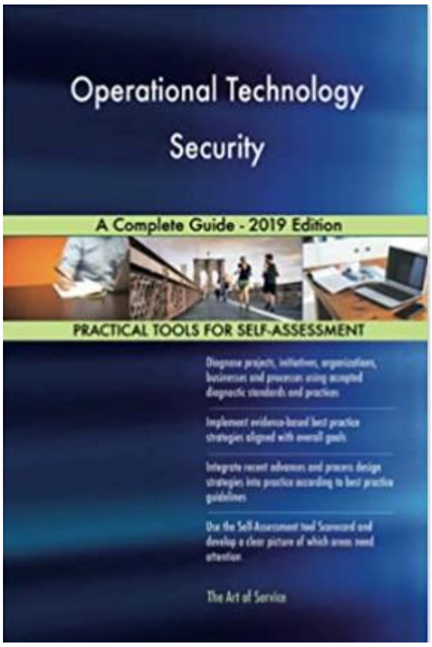
Unless you're talking a one-time, single-use project, there should be a process. That process needs to be designed by someone with a complex enough perspective to ask the right questions.

Authors/Editors: Gerardus Blokdyk (Author)

Year of issue: 2021

The book is available at the following link:

[https://www.amazon.com/Operational-Technology-Security-Complete-Guide/dp/0655829261](https://www.amazon.com/Operational-Technology-Security-Complete-Guide/dp/0655829261)


Operational Technology
Security
A Complete Guide - 2019 Edition
PRACTICAL TOOLS FOR SELF-ASSESSMENT
Diagnose projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices
Implement evidence-based best practice strategies aligned with overall goals
Integrate recent advances and process design strategies into practice according to best practice guidelines
Use the Self-Assessment tool Scorecard and develop a clear picture of which areas need attention
The Art of Service

## ICS security news selection

### Automotive Security Threats Are More Critical Than Ever

We've all marveled at the latest innovations from Tesla, the skill of Google's self-driving cars, or, at the very least, enjoyed playing a podcast on our phone through our car's speakers.

The automotive industry continues to innovate, bringing connectivity to vehicles in new ways from the cockpit to the engine. These new tools change the way people drive and view their cars. An automobile is no longer just for transportation from point A to point B, but cars are rolling data centers that transmit a wealth of actionable intelligence to the networks and systems around them. However, that same information is also a valuable commodity to hackers – who are looking to steal it at any cost. …

Source and more information:

https://www.securityweek.com/automotive-security-threats-are-more-critical-ever

### Critical Bug in Siemens SIMATIC PLCs Could Let Attackers Steal Cryptographic Keys

A vulnerability in Siemens Simatic programmable logic controller (PLC) can be exploited to retrieve the hard-coded, global private cryptographic keys and seize control of the devices.

"An attacker can use these keys to perform multiple advanced attacks against Siemens SIMATIC devices and the related TIA Portal, while bypassing all four of its access level protections," industrial cybersecurity company Claroty said in a new report.

"A malicious actor could use this secret information to compromise the entire SIMATIC S7-1200/1500 product line in an irreparable way." …

Source and more information:

https://thehackernews.com/2022/10/critical-bug-in-siemens-simatic-plcs.html

### Portnox introduces IoT fingerprinting and profiling solution to address rising IoT security threats

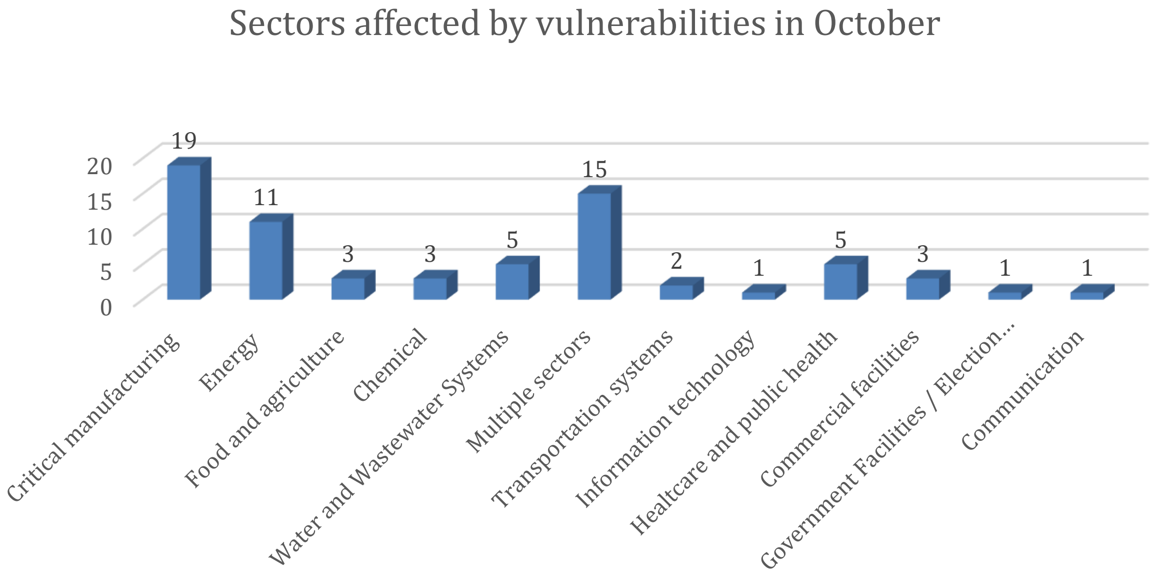
Portnox released a cloud-native IoT security solution to help mid-market and enterprise businesses address rising Internet of Things (IoT) security threats.

Now available via the Portnox Cloud, Portnox's new IoT fingerprinting and profiling capabilities empower organizations to identify, authenticate, authorize, and segment IoT devices across their network to ensure an effective zero trust security posture. …

https://www.helpnetsecurity.com/2022/10/13/portnox-iot-security-solution/

## ICS vulnerabilities

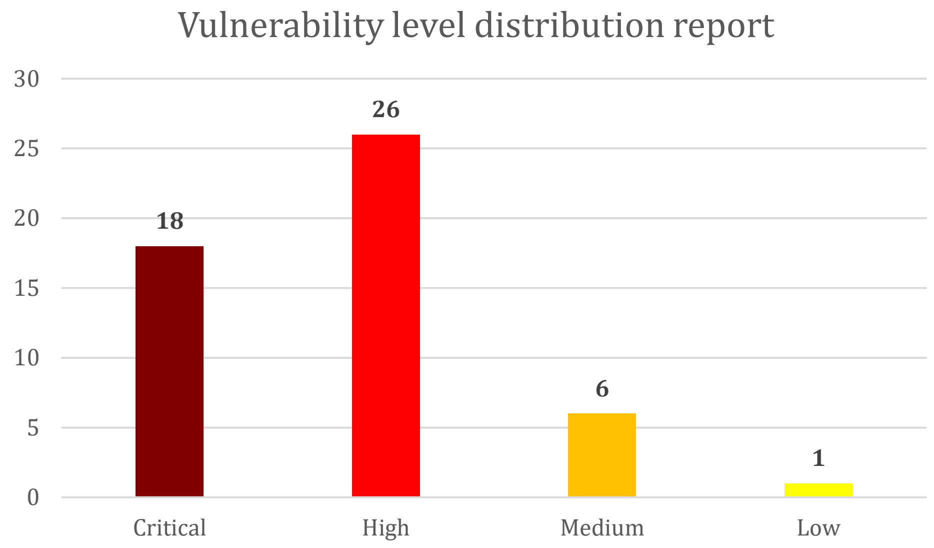
In October 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:



Average number of vulnerabilities per vulnerability report in October: **2,12**

The most common vulnerabilities in October:

| Vulnerability | CWE number | Piece |
|---|---|---|
| Improper Input Validation | CWE-20 | 6 |
| Cross-site Scripting | CWE-79 | 6 |
| Path Traversal | CWE-22 | 5 |
| Improper Access Control | CWE-284 | 5 |
| OS Command Injection | CWE-78 | 4 |



ICSA-22-221-01: **Mitsubishi Electric Multiple Factory Automation Products (Update C)**

**Critical** level vulnerabilities: Infinite Loop, OS Command Injection.

Mitsubishi Electric Multiple Factory Automation Products (Update C) | CISA

ICSA-22-300-01: **Rockwell Automation FactoryTalk Alarm and Events Server**

**High** level vulnerability: Improper Access Control.

Rockwell Automation FactoryTalk Alarm and Events Server | CISA

ICSA-22-300-02: **SAUTER Controls moduWeb**

**High** level vulnerability: Cross-site Scripting.

SAUTER Controls moduWeb | CISA

ICSA-22-300-03: **Rockwell Automation Stratix Devices Containing Cisco IOS**

**High** level vulnerabilities: Incorrect Authorization, Improper Input Validation, Improper Check for Unusual or Exceptional Conditions, Interpretation Conflict, OS Command Injection, Improper Verification of Cryptographic Signature, Path Traversal.

Rockwell Automation Stratix Devices Containing Cisco IOS | CISA

ICSA-22-300-04: **Trihedral VTScada**

**High** level vulnerability: Improper Input Validation.

Trihedral VTScada | CISA

ICSMA-22-298-01: **AliveCor KardiaMobile**

**Medium** level vulnerabilities: Authentication Bypass by Assumed-immutable Data, Missing Encryption of Sensitive Data.

AliveCor KardiaMobile | CISA

ICSA-22-298-01: **Haas Controller**

**Critical** level vulnerabilities: Missing Authentication for Critical Function, Insufficient Granularity of Access Control, Cleartext Transmission of Sensitive Information.

Haas Controller | CISA

ICSA-22-298-02: **HEIDENHAIN Controller TNC on HARTFORD Machine**

**High** level vulnerability: Improper Authentication.

HEIDENHAIN Controller TNC on HARTFORD Machine | CISA

ICSA-22-298-03: **Siemens Siveillance Video Mobile Server**

**Critical** level vulnerability: Weak Authentication.

Siemens Siveillance Video Mobile Server | CISA

ICSA-22-298-04: **Hitachi Energy MicroSCADA X DMS600**

**High** level vulnerability: Reliance on Uncontrolled Component.

Hitachi Energy MicroSCADA X DMS600 | CISA

ICSA-22-298-05: **Johnson Controls CKS CEVAS**

**Critical** level vulnerability: Cross-site Scripting.

Johnson Controls CKS CEVAS | CISA

ICSA-22-298-06: **Delta Electronics DIAEnergie**

**High** level vulnerabilities: Cross-site Scripting, SQL Injection.

Delta Electronics DIAEnergie | CISA

ICSA-22-298-07: **Delta Electronics InfraSuite Device Master**

**Critical** level vulnerabilities: Deserialization of Untrusted Data, Path Traversal, Missing Authentication for Critical Function.

Delta Electronics InfraSuite Device Master | CISA

ICSMA-20-296-02: **B. Braun SpaceCom, Battery Pack SP with Wi-Fi, and Data module compactplus (Update A)**

**High** level vulnerabilities: Cross-site Scripting, Open Redirect, XPath Injection, Session Fixation, Use of a One-way Hash without a Salt, Relative Path Traversal, Improper Verification of Cryptographic Signature, Improper Privilege Management, Use of Hard-coded Credentials, Active Debug Code, Improper Access Control.

B. Braun SpaceCom, Battery Pack SP with Wi-Fi, and Data module compactplus (Update A) | CISA

ICSA-22-293-01: **Bentley Systems MicroStation Connect**

**High** level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read.

Bentley Systems MicroStation Connect | CISA

ICSMA-21-294-01: **B. Braun Infusomat Space Large Volume Pump (Update A)**

**Critical** level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Cleartext Transmission of Sensitive Information, Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity, and Improper Input Validation.

B. Braun Infusomat Space Large Volume Pump (Update A) | CISA

ICSA-22-291-01: **Advantech R-SeeNet**

**Critical** level vulnerability: Path Traversal, Stack-based Buffer Overflow.

Advantech R-SeeNet | CISA

ICSA-21-287-03: **Mitsubishi Electric MELSEC iQ-R Series (Update A)**

**Critical** level vulnerability: Authorization Bypass Through User-controlled Key.

Mitsubishi Electric MELSEC iQ-R Series (Update A) | CISA

ICSA-22-286-01: **Siemens LOGO!**

**Medium** level vulnerability: Insufficient Verification of Data Authenticity.

Siemens LOGO! | CISA

ICSA-22-286-02: **Siemens Industrial Edge Management**

**High** level vulnerability: Improper Certificate Validation.

Siemens Industrial Edge Management | CISA

ICSA-22-286-03: **Siemens Solid Edge**

**High** level vulnerability: Heap-based Buffer Overflow.

Siemens Solid Edge | CISA

ICSA-22-286-04: **Siemens SIMATIC S7-1200 and S7-1500 CPU Families**

**Critical** level vulnerability: Insufficiently Protected Credentials.

Siemens SIMATIC S7-1200 and S7-1500 CPU Families | CISA

ICSA-22-286-05: **Hitachi Energy Lumada Asset Performance Management Prognostic Model Executor Service**

**High** level vulnerabilities: Allocation of Resources Without Limits or Throttling, Code injection.

Hitachi Energy Lumada Asset Performance Management Prognostic Model Executor Service | CISA

ICSA-22-286-06: **Siemens Desigo PXM Devices**

**High** level vulnerabilities: OS Command Injection, Exposure of Sensitive Information to an Unauthorized Actor, Cross-Site Scripting, Cross-Site Request Forgery, Improper Neutralization of Encoded URI Schemes in a Web Page, Execution with Unnecessary Privileges.

Siemens Desigo PXM Devices | CISA

ICSA-22-286-07: **Siemens Nucleus RTOS FTP Server**

**High** level vulnerability: Uncontrolled Resource Consumption.

Siemens Nucleus RTOS FTP Server | CISA

ICSA-22-286-08: **Siemens TCP Event Service of SCALANCE And RUGGEDCOM Devices**

**High** level vulnerability: Improper Input Validation.

Siemens TCP Event Service of SCALANCE And RUGGEDCOM Devices | CISA

ICSA-22-286-09: **Siemens SICAM P850 and P855 Devices**

**Critical** level vulnerabilities: Session Fixation, Improper Neutralization of Parameter/Argument Delimiters.

Siemens SICAM P850 and P855 Devices | CISA

ICSA-22-286-10: **Siemens JT Open Toolkit and Simcenter Femap**

**High** level vulnerability: Access of Uninitialized Pointer.

Siemens JT Open Toolkit and Simcenter Femap | CISA

ICSA-22-286-11: **Siemens SCALANCE and RUGGEDCOM Products**

**High** level vulnerability: Missing Authorization.

Siemens SCALANCE and RUGGEDCOM Products | CISA

ICSA-22-286-12: **Siemens APOGEE, TALON and Desigo PXC/PXM Products**

**Critical** level vulnerability: Uncontrolled Resource Consumption.

Siemens APOGEE, TALON and Desigo PXC/PXM Products | CISA

ICSA-22-286-13: **Siemens LOGO! 8 BM Devices**

**Critical** level vulnerabilities: Buffer Copy without Checking Size of Input; Improper Input Validation; Improper Validation of Specified Index, Position, or Offset in Input.

Siemens LOGO! 8 BM Devices | CISA

ICSA-22-286-14: **Siemens SIMATIC HMI Panels**

**High** level vulnerability: Improper Input Validation.

Siemens SIMATIC HMI Panels | CISA

ICSA-22-286-15: **Siemens SCALANCE X-200 and X-200IRT Families**

**High** level vulnerability: Cross-site Scripting.

Siemens SCALANCE X-200 and X-200IRT Families | CISA

ICSA-22-286-16: **Siemens Desigo CC and Cerberus DMS**

**Critical** level vulnerability: Use of Client-Side Authentication.

Siemens Desigo CC and Cerberus DMS | CISA

ICSA-21-250-01: **Mitsubishi Electric MELSEC iQ-R Series (Update A)**

**High** level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Insufficiently Protected Credentials, Overly Restrictive Account Lockout Mechanism.

Mitsubishi Electric MELSEC iQ-R Series (Update A) | CISA

ICSA-22-104-06: **Siemens PROFINET Stack Integrated on Interniche Stack (Update D)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

Siemens PROFINET Stack Integrated on Interniche Stack (Update D) | CISA

ICSA-22-069-03: **Siemens SINEC NMS (Update A)**

**High** level vulnerabilities: SQL Injection, Deserialization of Untrusted Data, Improper Privilege Management.

Siemens SINEC NMS (Update A) | CISA

ICSA-21-287-07: **Siemens SCALANCE (Update A)**

**Critical** level vulnerabilities: Cross-site Request Forgery, OS Command Injection, Classic Buffer Overflow, Command Injection, Path Traversal, Missing Encryption of Sensitive Data.

Siemens SCALANCE (Update A) | CISA

ICSA-21-315-06: **Siemens SCALANCE W1750D (Update A)**

**Critical** level vulnerabilities: Improper Restriction of Operations Within the Bounds of a Memory Buffer, Command Injection, Path Traversal.

Siemens SCALANCE W1750D (Update A) | CISA

ICSA-22-167-06: **Siemens Apache HTTP Server (Update A)**

**Critical** level vulnerabilities: NULL Pointer Dereference, Out-of-bounds Write, Server-side Request Forgery (SSRF).

Siemens Apache HTTP Server (Update A) | CISA

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

**High** level vulnerability: Infinite Loop.

Siemens OpenSSL Affected Industrial Products (Update D) | CISA

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

**Medium** level vulnerability: Null Pointer Dereference.

Siemens Industrial Products with OPC UA (Update C) | CISA

ICSA-22-284-01: **Altair HyperView Player**

**High** level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Use of Uninitialized Resource, Improper Validation of Array Index.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-284-01

ICSA-22-284-02: **Daikin Holdings Singapore Pte Ltd. SVMPC1 and SVMPC2**

**Critical** level vulnerabilities: Use of Hard-coded Password, Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-284-02

ICSA-22-284-03: **Sensormatic Electronics C-CURE 9000**

Low level vulnerability: Observable Response Discrepancy.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-284-03

ICSA-22-279-01: **Rockwell Automation FactoryTalk VantagePoint**

**Critical** level vulnerabilities: Improper Access Control, SQL Injection.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-279-01

ICSA-22-279-02: **HIWIN Robot System Software (HRSS)**

**High** level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-279-02

ICSMA-22-277-01: **BD Totalys MultiProcessor**

**Medium** level vulnerability: Use of Hard-coded Credentials.

BD Totalys MultiProcessor | CISA

ICSA-22-277-01: **Johnson Controls Metasys ADX Server**

**High** level vulnerability: Improper Authentication.

Johnson Controls Metasys ADX Server | CISA

ICSA-22-277-02: **Hitachi Energy Modular Switchgear Monitoring (MSM)**

**Medium** level vulnerabilities: Cross-Site Request Forgery (CSRF), HTTP Response Splitting.

Hitachi Energy Modular Switchgear Monitoring (MSM) | CISA

ICSA-22-277-03: **Horner Automation Cscape**

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

Horner Automation Cscape | CISA

ICSA-22-277-04: **OMRON CX-Programmer**

**High** level vulnerability: Out-of-bounds Write.

OMRON CX-Programmer | CISA

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

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

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

## ICS alerts

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

### Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.

This joint Cybersecurity Advisory (CSA) provides the APT actor's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified during the incident response activities by CISA and a third-party incident response organization. The CSA includes detection and mitigation actions to help organizations detect and prevent related APT activity. CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend the DIB sector and other critical infrastructure organizations implement the mitigations in this CSA to ensure they are managing and reducing the impact of cyber threats to their networks.

Source, the technical details and more information can be found on the website:

https://www.cisa.gov/uscert/ncas/alerts/aa22-277a