# 2022 May, 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.

! *From 2022 May the ICS security news selection replaced the Black Cell recommendations.* !

## List of Contents

# ICS good practices, recommendations

## Open-source tool for hardening commonly used HMI/SCADA system

There are some open-source free tools which can help to harden our HMI/SCADA systems. One of them is the GE CIMPLICITY Hardening Tool. The tool is capable to harden GE Digital's CIMPLICITY solution.

Otorio's researchers worked closely with GE Digital engineers to deliver a first of its kind open-source tool designed to identify GE CIMPLICITY misconfigurations.

The GE CIMPLICITY Hardening Tool verifies the security configuration of different CIMPLICITY components and helps operational teams ensure that the highest security standards are maintained. As an example, the tool checks for proper configuration of IPsec, which ensures secure communication between the different CIMPLICITY components.

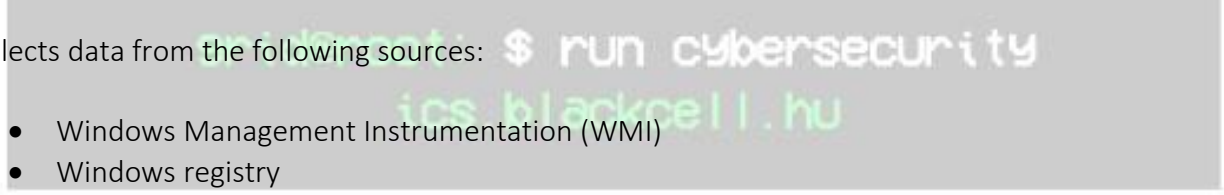
The hardening tool available on the following link:

https://github.com/otoriocyber/CIMPLICITY-Hardening-Tool

The hardening tool dependencies are:

The script is Powershell 2.0 compatible. Powershell >=2.0 is pre-installed on every Windows since Windows 7 and Windows Server 2008R2. The tool was tested on:

- Windows 7
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016




Collects data from the following sources:

- Windows Management Instrumentation (WMI)
- Windows registry
- Security Policy
- Netstat
- Dirlist
- Net and Netsh Commands

Further information clicks the links! Recommended to use the tool if your organization use GE Digital's CIMPLICITY solution!

Source and more information available on the following link:

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

## ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in June 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
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security
- 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.

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

### ICS Security Symposium

Public Safety Canada organized an ICS Security Symposium, where the main topic is the risk modelling. Risk Modelling in a security setting can be a nuanced process, and the cyber and physical aspects share a number of commonalities and differences. As these processes are often performed by separate divisions within security teams, we are seeking presentations that fit into this theme from both a cyber and physical point of view.

Topics should relate to risk modelling strategies and methodologies or may touch on subjects such as the various cyber and physical security risk modelling technologies, trends and lessons learned.

Virtually; June 7th – 8th, 2022

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/sympsm-en.aspx

### ICSICS 2022: 16. International Conference on 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 an exceptional value for students, academics and industry researchers.

International Conference on 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 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 Security of Industrial Control Systems.

Riga, Latvia; June 16th -17th, 2022

More details can be found on the following website:

https://waset.org/security-of-industrial-control-systems-conference-in-june-2022-in-riga

### ICISNS 2022: 16. International Conference on Industrial Security and Network Security (Paris)

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 Security and Network 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 Security and Network 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 Security and Network Security.

Paris, France; June 23rd – 24th, 2022

More details can be found on the following website:

https://waset.org/industrial-security-and-network-security-conference-in-june-2022-in-paris

### ICICSS 2022: 16. International Conference on Industrial Control Systems Security (Dubai)

It's the same conference as above, but hosted in Dubai instead of Paris.

Dubai, United Arab Emirates; June 27th -28th, 2022

More details can be found on the following website:

https://waset.org/industrial-control-systems-security-conference-in-june-2022-in-dubai

## ICS incidents

### US agricultural machinery maker AGCO hit by ransomware attack

AGCO announced that they suffered a ransomware attack in May that has impacted some of the company's production facilities.

While AGCO does not provide any details as to what is causing the disruption, the company likely shut down portions of its IT systems to prevent the attack's spread.

AGCO doesn't publish further information about the ransomware attack, but the organization's spokesperson said in a statement it expects operations at some facilities to be affected for "several days and potentially longer."

The ransomware attack comes at a time U.S. agricultural equipment makers were already facing persistent supply chain disruptions and labour strikes that left them unable to meet equipment demand from farmers.

US authorities recently warned of the risks of ransomware attacks against the US agriculture sector.

"The Federal Bureau of Investigation (FBI) is informing Food and Agriculture (FA) sector partners that ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss, and negatively impacting the food supply chain. The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer." reads the PIN alert published by the FBI. "Cyber actors may perceive cooperatives as lucrative targets with a willingness to pay due to the time sensitive role they play in agricultural production."

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

https://news.agcocorp.com/news/agco-announces-ransomware-attack

https://www.bleepingcomputer.com/news/security/us-agricultural-machinery-maker-agco-hit-by-ransomware-attack/

https://www.reuters.com/business/agco-says-some-production-facilities-hit-by-ransomware-attack-2022-05-06/

https://securityaffairs.co/wordpress/131058/cyber-crime/agco-suffered-ransomware-attack.html

# Book recommendation

## Industrial Automation and Control System Security Principles: Protecting the Critical Infrastructure

The use of cyber warfare as a prelude or substitute for kinetic attacks has gone from conjecture to reality. The obvious targets of such assaults are a nation's defense establishment, critical infrastructure, corporate intellectual property, government databases, and industrial capabilities. Contrary to popular opinion, there are effective, structured defenses against such aggression, if they are properly implemented and maintained.

This text builds on the established fundamentals of information system security, examines the existing and emerging standards and guidelines from a variety of respected sources, and addresses the unique requirements of industrial automation and control systems. It presents a clear and implementable formula to defend crucial elements, such as refineries, chemical plants, manufacturing operations, power plants, transportation systems, and pipelines. This work develops a novel protection approach based on the merging of the best relevant and proven government and industry standards, resulting in a practical instrument that can be straightforwardly applied to secure our valuable resources.

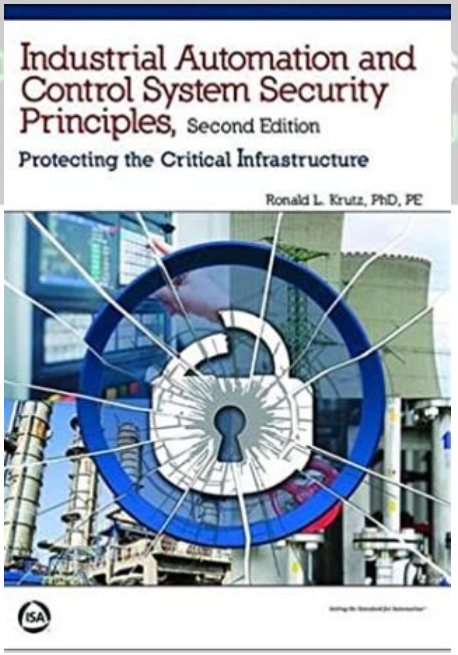
Authors/Editors: Ronald L. Krutz, PhD, PE

Year of issue: 2017

The book is available at the following links:

https://www.amazon.com/Industrial-Automation-Control-Security-Principles/dp/1937560635

https://www.isa.org/getmedia/82d1c490-2dd5-4621-9ea4-21f637ab34c3/IACS_SecondEd_Krutz_chapter_3.pdf



## ICS security news selection

### Vulnerable Today, Hacked Tomorrow: How a Lack of OT Cybersecurity Affects Critical Infrastructure

Did you know that almost 50% of ICS (Industrial Control Systems) organizations don't have dedicated 24/7
security to manage Operational Technology (OT) incidents should a cyber event occur? While this fact may not be common knowledge to organizations, hackers have been readily exploiting this gap, as seen in incidents such as the Colonial Pipeline shutdown or the Oldsmar, Florida water treatment plant breach. Adversaries have learned that targeting ICS can result in quicker and higher payouts because of the potential to disrupt operations, prompting threat actors to focus on ICS targets. Ransomware attacks have proven very effective for OT systems just as with IT systems and are now being used as a weapon in international politics.

Source and more information:
https://cyberdefensemagazine.tradepub.com/free/w_cyba137/

### Russia-Linked Pipedream/Incontroller ICS Malware Designed to Target Energy Facilities

The US government and cybersecurity firms on Wednesday released details about a new piece of malware designed to manipulate and disrupt industrial processes by hacking industrial control systems (ICS).

The malware, described as a modular ICS attack framework and a collection of custom-made tools, can be used by threat actors to target ICS and SCADA devices, including programmable logic controllers (PLCs) from Schneider Electric and Omron, and OPC UA servers.

Source and more information:
https://www.securityweek.com/russia-linked-pipedreamincontroller-ics-malware-designed-target-energy-facilities

### Mitsubishi Electric faked safety and quality control tests for decades

Mitsubishi Electric, one of the world's leading manufacturers of large-scale electrical and HVAC systems has admitted to fraudulently conducting quality assurance tests on its transformers—for decades.

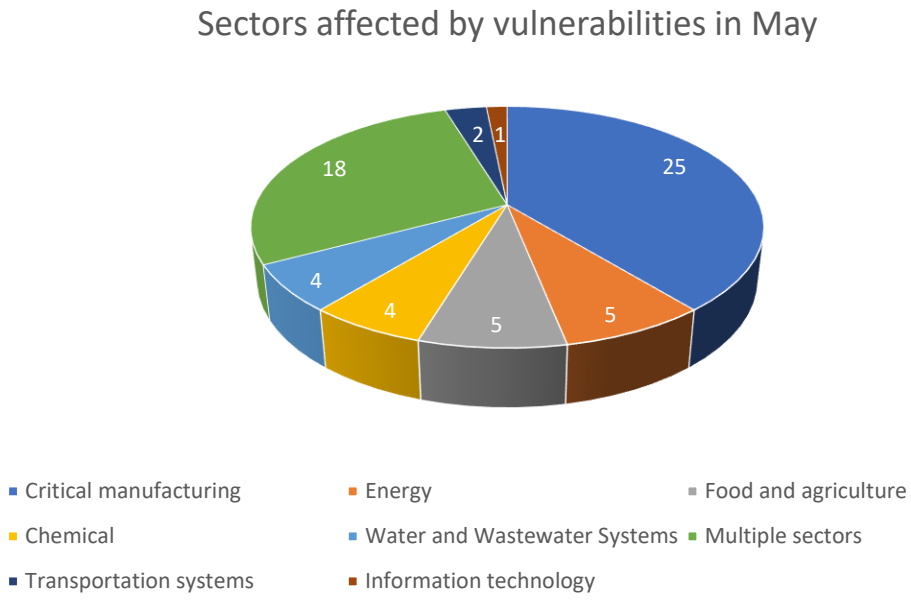
Thousands of such improperly tested transformers were then shipped both within Japan and overseas.

And it turns out, this isn't the first time Mitsubishi has been caught cheating either.

Source and more information:
https://www.bleepingcomputer.com/news/technology/mitsubishi-electric-faked-safety-and-quality-control-tests-for-decades/

## ICS vulnerabilities

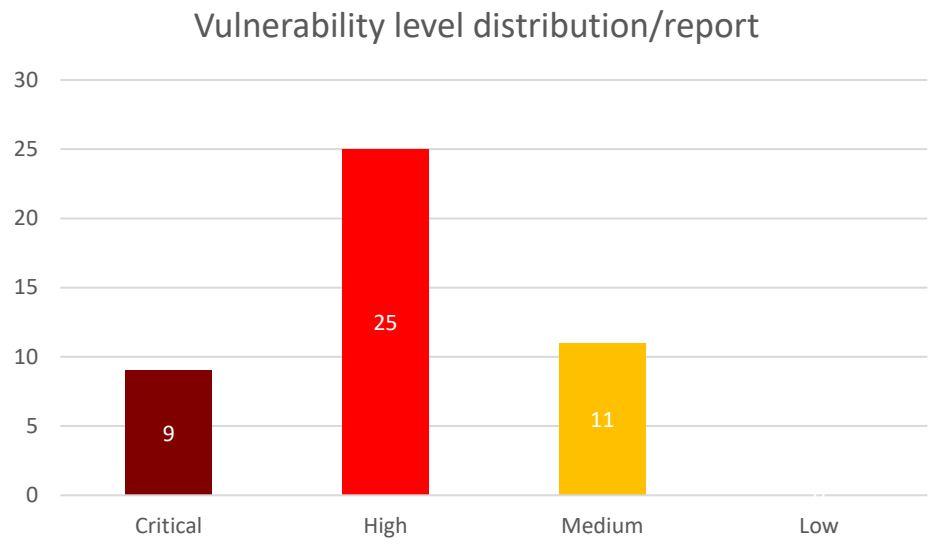
In May 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:




Average number of vulnerabilities per vulnerability report in May: 2,33

The most common vulnerabilities in May:

| Vulnerability | CWE number | Piece |
|---|---|---|
| Uncontrolled Resource Consumption | CWE-400 | 6 |
| NULL Pointer Dereference | CWE-476 | 5 |
| Out-of-bounds Read | CWE-125 | 5 |
| Cross-site Scripting | CWE-79 | 5 |
| Improper Input Validation | CWE-20 | 4 |
| Out-of-bounds Write | CWE-787 | 4 |
| Improper Authentication | CWE-287 | 3 |
| Path Traversal | CWE-22 | 3 |
| Heap-based Buffer Overflow | CWE-122 | 3 |
| Stack-based Buffer Overflow | CWE-121 | 3 |




ICSA-22-146-01: Keysight N6854A Geolocation server and N6841A RF Sensor software
Critical level vulnerabilities: Relative Path Traversal, Deserialization of Untrusted Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-146-01

ICSA-22-146-02: Horner Automation Cscape Csfont
High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Heap-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-146-02

ICSA-22-144-01: Rockwell Automation Logix Controllers
Medium level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-01

ICSA-22-144-02: Matrikon OPC Server
Medium level vulnerability: Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-144-02

ICSA-21-049-02: Mitsubishi Electric FA Engineering Software Products (Update E)
High level vulnerabilities: Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-049-02

ICSA-20-212-04: Mitsubishi Electric Factory Automation Engineering Products (Update G)
High level vulnerability: Unquoted Search Path or Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-04

ICSA-22-139-01: Mitsubishi Electric MELSEC iQ-F Series
High level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-139-01

ICSA-22-137-01: Circutor COMPACT DC-S BASIC

Medium level vulnerability: Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-137-01

ICSA-22-132-01: **Delta Electronics CNCSoft**
High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-01

ICSA-22-132-02: **Mitsubishi Electric MELSOFT iQ AppPortal**
Critical level vulnerabilities: Missing Authorization, Out-of-bounds Write, NULL Pointer Dereference, Classic Buffer Overflow, HTTP Request Smuggling, Infinite Loop.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-02

ICSA-22-132-03: **Inkscape in Industrial Products**
High level vulnerabilities: Out-of-bounds Read, Access of Uninitialized Pointer, Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-03

ICSA-22-132-04: **Cambium Networks cnMaestro**
Critical level vulnerabilities: OS Command Injection, SQL Injection, Path Traversal, Use of Potentially Dangerous Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-04

ICSA-22-132-05: **Siemens Industrial PCs and CNC devices**
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-22-132-06: **Siemens SIMATIC WinCC**
High level vulnerability: Insecure Default Initialization of Resource.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-06

ICSA-22-132-07: **Siemens SICAM P850 and SICAM P855**
Critical level vulnerabilities: Improper Neutralization of Parameter/Argument Delimiters, Cleartext Transmission of Sensitive Information, Cross-site Scripting, Missing Authentication for Critical Function, Authentication Bypass by Capture-replay, Improper Authentication.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-07

ICSA-22-132-08: **Siemens Industrial Products with OPC UA**
Medium level vulnerability: Null Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-08

ICSA-22-132-09: **Siemens JT2GO and Teamcenter Visualization**
High level vulnerabilities: Infinite Loop, Null Pointer Dereference, Integer Overflow to Buffer Overflow, Double Free, Access of Uninitialized Pointer.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-09

ICSA-22-132-10: **Siemens Desigo PXC and DXR Devices**

Critical level vulnerabilities: Special Element Injection, Uncontrolled Resource Consumption, Use of Password Hash with Insufficient Computational Effort, Insufficient Session Expiration, Observable Discrepancy, Improper Restriction of Excessive Authentication Attempts, Sensitive Cookie in HTTPS Session Without 'Secure' Attribute, Uncaught Exception.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-10

ICSA-22-132-11: Siemens SIMATIC CP 44x-1 RNA
High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-11

ICSA-22-132-12: Siemens Industrial Products
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-22-132-13: Siemens Industrial Devices using libcurl
High level vulnerability: Use After Free.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-13

ICSA-22-132-14: Siemens Simcenter Femap
High level vulnerability: Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-14

ICSA-22-132-15: Siemens OpenV2G
Medium level vulnerability: Classic Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-15

ICSA-22-132-16: Siemens Teamcenter
High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-132-16

ICSA-22-104-05: Siemens OpenSSL Vulnerabilities in Industrial Products (Update A)
Medium level vulnerability: NULL Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-104-05

ICSA-22-102-04: Mitsubishi Electric GT25-WLAN (Update A)
Medium level vulnerabilities: Improper Removal of Sensitive Information Before Storage or Transfer, Inadequate Encryption Strength, Missing Authentication for Critical Function, Injection, Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-102-04

ICSA-22-041-02: Siemens SIMATIC WinCC and PCS (Update B)
Medium level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Insertion of Sensitive Information into Externally-Accessible File or Directory.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-02

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

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

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

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

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

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

ICSA-21-159-13: Siemens SIMATIC RFID (Update B)

High level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-159-13

ICSA-20-105-06: Siemens SIMOTICS, Desigo, APOGEE, and TALON (Update D)

High level vulnerability: Business Logic Errors.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-06

ICSA-20-105-07: Siemens SCALANCE and SIMATIC (Update H)

High level vulnerability: Resource Exhaustion.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-07

ICSA-20-014-05: Siemens TIA Portal (Update D)

High level vulnerability: Path Traversal.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-05

ICSA-19-253-03: Siemens Industrial Products (Update R)

High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-19-253-03

ICSA-22-130-01: Adminer in Industrial Products

High level vulnerability: Files or Directories Accessible to External Parties.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-01

ICSA-22-130-02: Eaton Intelligent Power Protector

Medium level vulnerability: Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-02

ICSA-22-130-03: Eaton Intelligent Power Manager Infrastructure

Medium level vulnerabilities: Cross-site Scripting, Reflected Cross-site Scripting, Improper Neutralization of Formula in a CSV File.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-03

ICSA-22-130-04: **Eaton Intelligent Power Manager**
Medium level vulnerability: Cross-site Scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-04

ICSA-22-130-05: **AVEVA InTouch Access Anywhere and Plant SCADA Access Anywhere**
High level vulnerability: Exposure of Resource to Wrong Sphere.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-05

ICSA-22-130-06: **Mitsubishi Electric MELSOFT GT OPC UA**
High level vulnerabilities: Out-of-bounds Read, Integer Overflow or Wraparound.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-130-06

ICSA-22-125-01: **Johnson Controls Metasys**
High level vulnerability: Unverified Password Change.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-125-01

ICSA-22-123-01: **Yokogawa CENTUM and ProSafe-RS**
High level vulnerabilities: OS Command Injection, Improper Authentication, NULL Pointer Dereference, Improper Input Validation, Resource Management Errors.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-123-01

ICSA-22-118-01: **Johnson Controls Metasys**
High level vulnerability: Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-118-01

ICSA-22-081-01: **Delta Electronics DIAEnergie (Update B)**
Critical level vulnerabilities: Path Traversal, Incorrect Default Permissions, SQL Injection, Uncontrolled Search Path Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01



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 May 2022, ICS-CERT has not published alerts.