

2021. 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, furthermore 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 cara@blackcell.hu.

List of Contents

<u>ICS GOOD PRACTICES, RECOMMENDATIONS</u>	2
<u>ICS TRAININGS, EDUCATION</u>	3
<u>ICS CONFERENCES</u>	6
<u>ICS INCIDENTS</u>	8
<u>BOOK RECOMMENDATION</u>	10
<u>BLACK CELL RECOMMENDATIONS</u>	11
<u>ICS VULNERABILITIES</u>	12
<u>ICS ALERTS</u>	18

ICS good practices, recommendations

Design principles and Operational Technology

The National Cyber Security Centre (UK) published a guidance, which describes the Design principles and Operational Technology. If an organization wants to establish and maintain a robust and resilient Operational Technology, this guidance is helpful.

The guidance shows a case study with important principles and operational activities, which are the following:

1. Establish the context before designing a system
“Determine all the elements which compose your system, so your defensive measures will have no blind spots.” (Attack trees, Network zoning, Critical Zone Boundaries, Supply chain security, Network design and documentation, A simple network diagram)
2. Make compromise difficult
“An attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible.” (Do not trust external input, Enforce one way flow, Reduce the attack surface, Gain confidence in crucial security controls)
3. Make disruption difficult
“Design a system that is resilient to denial of service attacks and usage spikes”
4. Making compromise detection easier
“Design your system so you can spot suspicious activity as it happens and take necessary action” (Collecting logs, Detecting malware, Keep the attacker in the dark, Simple communication, Access to the Process Control System (PCS), Detecting attacks against the PCS)
5. Reducing the impact of compromise
“If an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible” (Only the essentials, Administration, Allowing for a smooth recovery, Cost analysis, Separation of duties, Protecting documentation)

Read the guidance carefully and analyse the gaps. If one or more things missing, try to fill the gaps.

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

<https://www.ncsc.gov.uk/collection/cyber-security-design-principles/examples/study-operational-tech>

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in June 2021:

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

<https://www.sans.org/course/ics-scada-cyber-security-essentials#results>

Periodic online courses:

The Coursera (<https://www.coursera.org/>) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization
- Industrial IoT on Google Cloud Platform **New**
- Emerging Technologies: From Smartphones to IoT to Big Data Specialization **New**
- CAD and Digital Manufacturing Specialization **New**

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
- 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

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
 - o 07-12. June 2021.
 - o 14-19. June 2021.
 - o anytime, on demand.
- ICS515: ICS Active Defense and Incident Response
 - o 07.11. June 2021.
 - o 14-18. June 2021.
 - o 28-02. June-July 2021.
 - o 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

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/>

SCADAhacker-com website provides ICS security online courses:

- Understanding, Assessing and Securing Industrial Control Systems

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, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

<https://scadahacker.com/training.html>

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the “Certified SCADA Security Architect” certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

<https://www.infosecinstitute.com/courses/scada-security-boot-camp/>

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a 3 Days Course, which is designed for:

- o IT and ICS cybersecurity personnel
- o Field support personnel and security operators
- o Auditors, vendors and team leaders
- o Electric utility engineers
- o System personnel & System operators
- o Independent system operator personnel
- o Electric utility personnel involved with ICS security.
- o Technicians, operators, and maintenance personnel
- o Investors and contractors in electric industry
- o 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/>

ICS conferences

In June 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

Industrial Control Systems Joint Working Group (ICSJWG)

The Cybersecurity and Infrastructure Security Agency (CISA) hosts the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems.

The ICSJWG provides a vehicle for communicating and partnering across all Critical Infrastructure (CI) Sectors between federal agencies and departments, as well as private asset owners/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the collaborative efforts of the industrial control systems stakeholder community in securing CI by accelerating the design, development, and deployment of secure industrial control systems.

Webinar, virtual meeting; 2. June 2021.;

More details can be found on the following website:

<https://us-cert.cisa.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>

Industrial Control Systems (ICS) Cyber Security Conference

The SecurityWeeks 2021 ICS Cyber Security Conference will be held at the InterContinental Atlanta with content available online as a hybrid event in SecurityWeek's virtual conference environment.

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.

Online event; 22-24. June 2021.

More details can be found on the following website:

<https://www.icscybersecurityconference.com/>

International Conference on Industrial Control Systems Security ICICSS

15. International Conference on Industrial Control Systems Security aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences and research results on all aspects of Industrial Control Systems Security. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the

most recent innovations, trends, and concerns as well as practical challenges encountered, and solutions adopted in the fields of Industrial Control Systems Security.

Dubai, United Arab Emirates; 29-30. June 2021.

More details can be found on the following website:

<https://waset.org/industrial-control-systems-security-conference-in-june-2021-in-dubai>



ICS incidents

Cring ransomware disrupted production at two manufacturing sites in Italy

Last month Kaspersky reported a ransomware attack, what hit the production at two manufacturing sites in Italy. According to the report “The servers with the databases required for production were encrypted,”.

The hackers used a variant of Cring ransomware mentioned the report. Details on other victims were not immediately available. Kaspersky informed the public, that the hackers exploited old vulnerabilities in virtual private networking software made by California-based security vendor Fortinet.

Nowadays the hackers focus on the vaccine manufacturers increasingly, but the critical infrastructures, the vital services and the manufacturers are also potential victims as usual.

The following website detailed the exploitation of the vulnerability:

https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/#_Toc67921522

ComputerWeekly.com news informed, that the bug was 2 years old and many other manufacturers suffered a Cring ransomware attack due to the CVE-2018-13379 vulnerability.

Arstechnica.com said that “Incident responders eventually restored most but not all of the encrypted data from backups. The victim didn’t pay any ransom. There are no reports of the infections causing harm or unsafe conditions.”

Sources and more details can be found on the following websites:

https://www.cyberscoop.com/ransomware-industrial-europe-kaspersky-cring/?category_news=news *

https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/#_Toc67921522

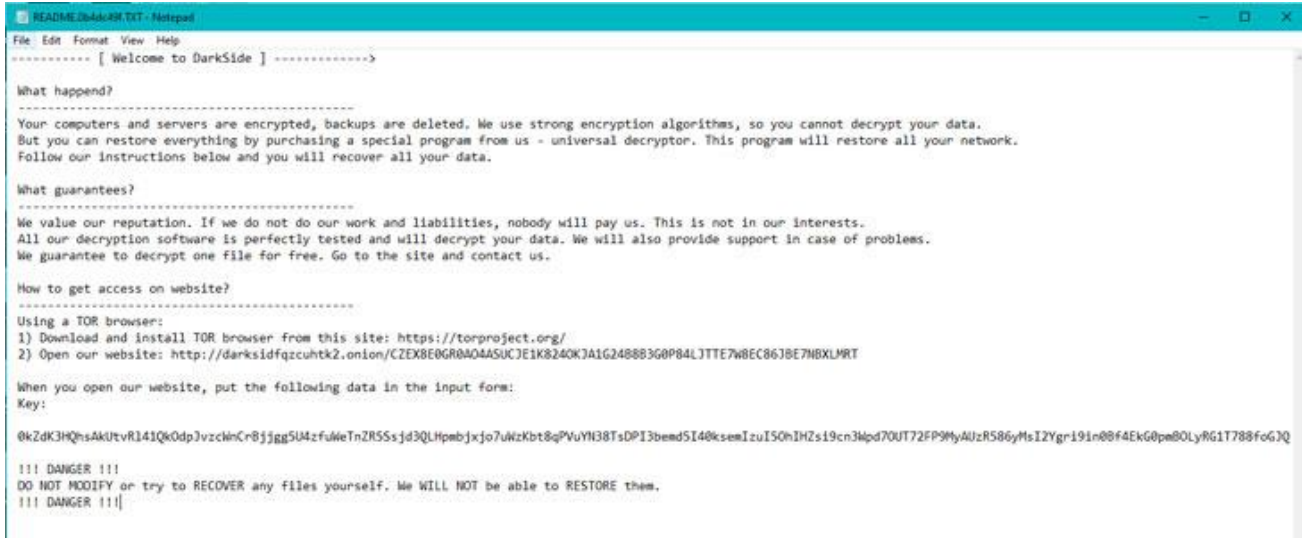
<https://arstechnica.com/information-technology/2021/04/ransomware-shuts-down-production-at-two-manufacturing-plants/>



US. fuel pipeline attacked with ransomware

Colonial Pipeline Company which is a gas and fuel and gasoline supplier company, suffered a cyberattack on the on 7th of May. As reported, a ransomware (Darkside) caused the infrastructure to shut down.

Darkside ransom note:



* An analysis said that this kind of ransomware targeted the English-speaking firms and countries. In 2020, the ransomware stole 100 GB of data from 40 different organizations according to Bloomberg's report. The attackers presumably use the earlier stolen data in this attack.

The attacked has shut down about 5500 miles of pipeline operation. According to the open-source information the vulnerability of aging infrastructure that has been connected, directly or indirectly, to the internet.

Colonial Pipeline Company paid 4,4 million dollars to the hackers.

“Colonial Pipeline is taking steps to understand and resolve the issue,” the company said. “Our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation.”

No further technical information was released about the attack. The number of cyberattacks against critical infrastructure increased especially in the G20 countries. There are many ransomware that uses different vulnerabilities, so when a data breach turns out, the affected firms must react accordingly.

Sources and more details can be found on the following websites:

<https://thehackernews.com/2021/05/ransomware-cyber-attack-forced-largest.html> *

<https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html>

<https://www.theverge.com/2021/5/19/22443933/colonial-pipeline-ransom-4-million-hack-gas-shortage>

Book recommendation

Cybersecurity for SCADA Systems, 2nd Edition

A general background of SCADA system technology and cybersecurity concepts and technologies, showing how the two can be brought together to safeguard our infrastructure and computer automation systems. This book provides a high-level overview of this unique technology, with an explanation of each market segment. Readers will understand the vital issues and learn strategies for decreasing or eliminating system vulnerabilities.

The world has changed since the first edition was published in 2006. There have been many technological changes in communications and networking and in other areas of computer science. More focus is given to implementing cybersecurity protections and technical countermeasures. The second edition also takes advantage of the evolved industry-specific cybersecurity standards that have emerged, especially in the electric power and oil-and-gas pipeline industry sectors.

Features and Benefits

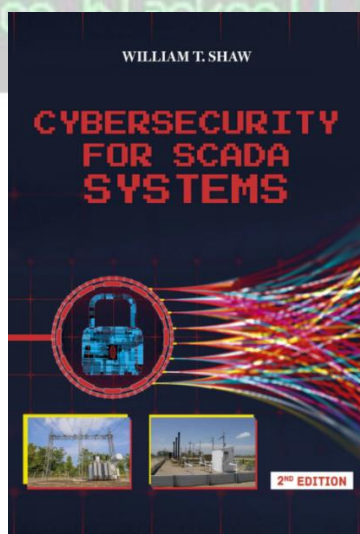
- Functional breakdown and explanation of the typical features, capabilities, and components of a SCADA system
- IT and cybersecurity technology and terminology overview and explanation
- Industry-specific as well as generalized discussion of SCADA vulnerabilities and available remediation strategies
- Discussion of physical and electronic security issues and strategies

Authors/Editors: Dr. William (Tim) Shaw - CISSP, C|EH, CPT, CAP

Year of issue: 2021.

The book available at the following link:

<https://www.pennwellbooks.com/cybersecurity-for-scada-systems-2nd-edition/>



Black Cell recommendations

Lessons from 2020: Defeating Targeted Ransomware Attacks at Industrial Sites

Waterfall published an information sheet with a hot topic: ransomware attacks against ICS systems lessons learned from 2020.

The sheet mentioned the SolarWinds Orion / SUNBURST data breach and some details from these breaches. It also mentioned Cloud connectivity and IIoT relevance in this issue. The importance of supply chain attacks is also described well.

The sheet describes the growing numbers of IT and OT ransomware attacks and give some insight to the threat environment.

The reader meets the conclusions and some tips for what to do to prevent these ransomware attacks in the industrial operation sites.

We recommend reading this information sheet and recommend to think through the statements. Try to evaluate our risk assessment and identify the gaps. The prevention is always a cheaper solution than the reaction.

The related sheet is available at the following link:

https://us-cert.cisa.gov/sites/default/files/ICSJWG-Archive/QLN_MAR_21/ICS_Ransomware_ICSJWG_Waterfall_Security_FINAL_S508C.pdf



```
grid@root: $ run cybersecurity  
ics.blackcell.hu
```

ICS vulnerabilities

In May 2021, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSA-21-147-01: GENIVI Alliance DLT

Critical level vulnerability: Heap-based Buffer Overflow.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-147-01>

ICSA-21-147-02: Johnson Controls Sensormatic Electronics VideoEdge

High level vulnerability: Off-by-one Error.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-147-02>

ICSA-21-147-03: MesaLabs AmegaView

Critical level vulnerabilities: Command Injection, Improper Authentication, Authentication Bypass Using an Alternate Path or Channel, Improper Privilege Management.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-147-03>

ICSA-21-147-04: Siemens JT2Go and Teamcenter Visualization

High level vulnerabilities: Untrusted Pointer Dereference, Out-of-bounds Read, Stack-based Buffer Overflow.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-147-04>

ICSA-21-147-05: Mitsubishi Electric MELSEC iQ-R Series

Medium level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-147-05>

ICSA-21-049-02: Mitsubishi Electric FA engineering software products (Update A)

High level vulnerabilities: Heap-based Buffer Overflow, Improper Handling of Length Parameter Inconsistency.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-049-02>

ICSA-21-040-06: Siemens JT2Go and Teamcenter Visualization (Update A)

High level vulnerabilities: Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer overflow, Out-of-Bounds Write, Type Confusion, Untrusted Pointer Dereference, Incorrect Type Conversion or Cast.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-040-06>

ICSA-21-012-03: Siemens JT2Go and Teamcenter Visualization (Update B)

High level vulnerabilities: Type Confusion, Improper Restriction of XML External Entity Reference, Out-of-Bounds Write, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Out-of-Bounds Read.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-012-03>

ICSA-20-212-03: Mitsubishi Electric Factory Automation Products Path Traversal (Update B)

High level vulnerability: Path Traversal.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-212-03>

ICSA-20-212-04: **Mitsubishi Electric Factory Automation Engineering Products (Update C)**

High level vulnerability: Unquoted Search Path or Element.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-212-04>

ICSA-21-145-01: **Datakit Libraries bundled in Luxion KeyShot**

High level vulnerabilities: Out-of-bounds Write, Exposure of Sensitive Information to an Unauthorized Actor, Stack-Based buffer Overflow, Untrusted Pointer Dereference, Out-of-bounds Read.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-145-01>

ICSA-21-145-02: **Rockwell Automation Micro800 and MicroLogix 1400**

Medium level vulnerability: Channel Accessible by Non-endpoint.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-145-02>

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

Critical level vulnerability: Integer Overflow or Wraparound.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04>

ICSA-21-138-01: **Emerson Rosemount X-STREAM**

High level vulnerabilities: Inadequate Encryption Strength, Unrestricted Upload of File with Dangerous Type, Path Traversal, Use of Persistent Cookies Containing Sensitive Information, Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-138-01>

ICSA-21-021-04: **Mitsubishi Electric MELFA (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-021-04>

ICSA-20-324-05: **Mitsubishi Electric MELSEC iQ-R Series (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-324-05>

ICSA-20-303-01: **Mitsubishi Electric MELSEC iQ-R, Q and L Series (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-303-01>

ICSA-20-282-02: **Mitsubishi Electric MELSEC iQ-R Series (Update C)**

High level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-282-02>

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

High level vulnerability: Predictable Exact Value from Previous Values.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-245-01>

ICSA-21-133-01: Rockwell Automation Connected Components Workbench

High level vulnerabilities: Deserialization of Untrusted Data, Path Traversal, Improper Input Validation.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-133-01>

ICSA-21-133-02: Johnson Controls Sensormatic Tyco AI

High level vulnerability: Off-by-one Error.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-133-02>

ICSA-21-133-03: OPC Foundation UA Products Built with .NET Framework

High level vulnerability: Uncontrolled Recursion.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-133-03>

ICSA-21-133-04: OPC UA Products Built with the .NET Framework 4.5, 4.0, and 3.5

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

<https://us-cert.cisa.gov/ics/advisories/icsa-21-133-04>

ICSA-21-131-01: Omron CX-One

High level vulnerability: Stack-based Buffer Overflow.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-01>

ICSA-21-131-02: Mitsubishi Electric GOT and Tension Controller

Medium level vulnerability: Buffer Access with Incorrect Length Value.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-02>

ICSA-21-131-03: Siemens Linux Based Products

High level vulnerability: Use of Insufficiently Random Values.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-03>

ICSA-21-131-04: Siemens SINAMICS Medium Voltage Products

High level vulnerability: Missing Authentication for Critical Function.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-04>

ICSA-21-131-05: Siemens Mendix Database Replication Module

Low level vulnerability: Generation of Error Message Containing Sensitive Information.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-05>

ICSA-21-131-06: Siemens SNMP Implementation of WinCC Runtime

Medium level vulnerability: Out-of-bounds Write.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-06>

ICSA-21-131-07: Siemens SIMATIC NET CP343-1

High level vulnerability: Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-07>

ICSA-21-131-08: **Siemens Tecnomatix Plant Simulation**

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-08>

ICSA-21-131-09: **Siemens Mendix Excel Importer Module**

Low level vulnerability: Generation of Error Message Containing Sensitive Information.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-09>

ICSA-21-131-10: **Siemens SCALANCE XM-400 and XR-500 Devices**

High level vulnerability: Incorrect Calculation.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-10>

ICSA-21-131-11: **Siemens SIMATIC UltraVNC HMI WinCC Products**

Critical level vulnerabilities: Improper Initialization, Out-of-bounds Read, Heap-based Buffer Overflow, Stack-based Buffer Overflow, Access of Memory Location After End of Buffer, Improper Null Termination.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-11>

ICSA-21-131-12: **Siemens SIMATIC SmartVNC HMI WinCC Products**

Critical level vulnerabilities: Access of Memory Location After End of Buffer, Improper Handling of Exceptional Conditions, Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-12>

ICSA-21-131-13: **Siemens SINAMICS Medium Voltage Products**

High level vulnerability: Missing Authentication for Critical Function.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-13>

ICSA-21-131-14: **Siemens SCALANCE W1750D**

Critical level vulnerabilities: Improper Authentication, Classic Buffer Overflow, Command Injection, Improper Input Validation, Race Condition, Cross-site Scripting.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-14>

ICSA-21-131-15: **Siemens SIMATIC S7-1500**

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

<https://us-cert.cisa.gov/ics/advisories/icsa-21-131-15>

ICSA-21-068-06: **Siemens TCP/IP Stack Vulnerabilities—AMNESIA:33 in SENTRON PAC / 3VA Devices (Update A)**

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

<https://us-cert.cisa.gov/ics/advisories/icsa-21-068-06>

ICSA-21-068-10: **Siemens SCALANCE and SIMATIC libcurl (Update A)**

High level vulnerability: Out-of-bounds Read.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10>

ICSA-21-040-08: **Siemens SIMARIS Configuration (Update A)**

Low level vulnerability: Incorrect Default Permissions.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-040-08>

ICSA-20-343-02: **Mitsubishi Electric GOT and Tension Controller (Update A)**

High level vulnerability: Out-of-bounds Read.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-343-02>

ICSA-20-343-08: **Siemens Products using TightVNC (Update A)**

No available information about the vulnerability score. Heap-based Buffer Overflow, Null Pointer Dereference, Buffer Copy Without Checking Size of Input.

<https://us-cert.cisa.gov/ics/advisories/icsa-20-343-08>

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

High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.

<https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03>

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

Critical level vulnerability: Integer Overflow or Wraparound.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04>

ICSA-21-047-01: **Open Design Alliance Drawings SDK (Update A)**

High level vulnerabilities: Stack-based Buffer Overflow, Type Confusion, Untrusted Pointer Dereference, Incorrect Type Conversion or Cast, Memory Allocation with Excessive Size Value, Out of Bounds Write.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-047-01>

ICSA-21-124-01: **Advantech WISE-PaaS RMM**

Critical level vulnerability: Use of Hard-coded Credentials.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-124-01>

ICSA-21-124-02: **Delta Electronics CNCSoft ScreenEditor**

High level vulnerability: Out-of-bounds Write.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-124-02>

ICSA-21-119-01: **Texas Instruments SimpleLink**

Critical level vulnerabilities: Stack-based Buffer Overflow, Integer Overflow or Wraparound.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-01>

ICSA-21-119-02: **Cassia Networks Access Controller**

Medium level vulnerability: Path Traversal.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-02>

ICSA-21-119-03: Johnson Controls Exacq Technologies exacqVision

High level vulnerability: Off-by-one Error.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-03>

ICSA-21-119-04: **Multiple RTOS**

Critical level vulnerability: Integer Overflow or Wraparound.

<https://us-cert.cisa.gov/ics/advisories/icsa-21-119-04>

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 2021, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

<https://www.us-cert.gov/ics/alerts>

