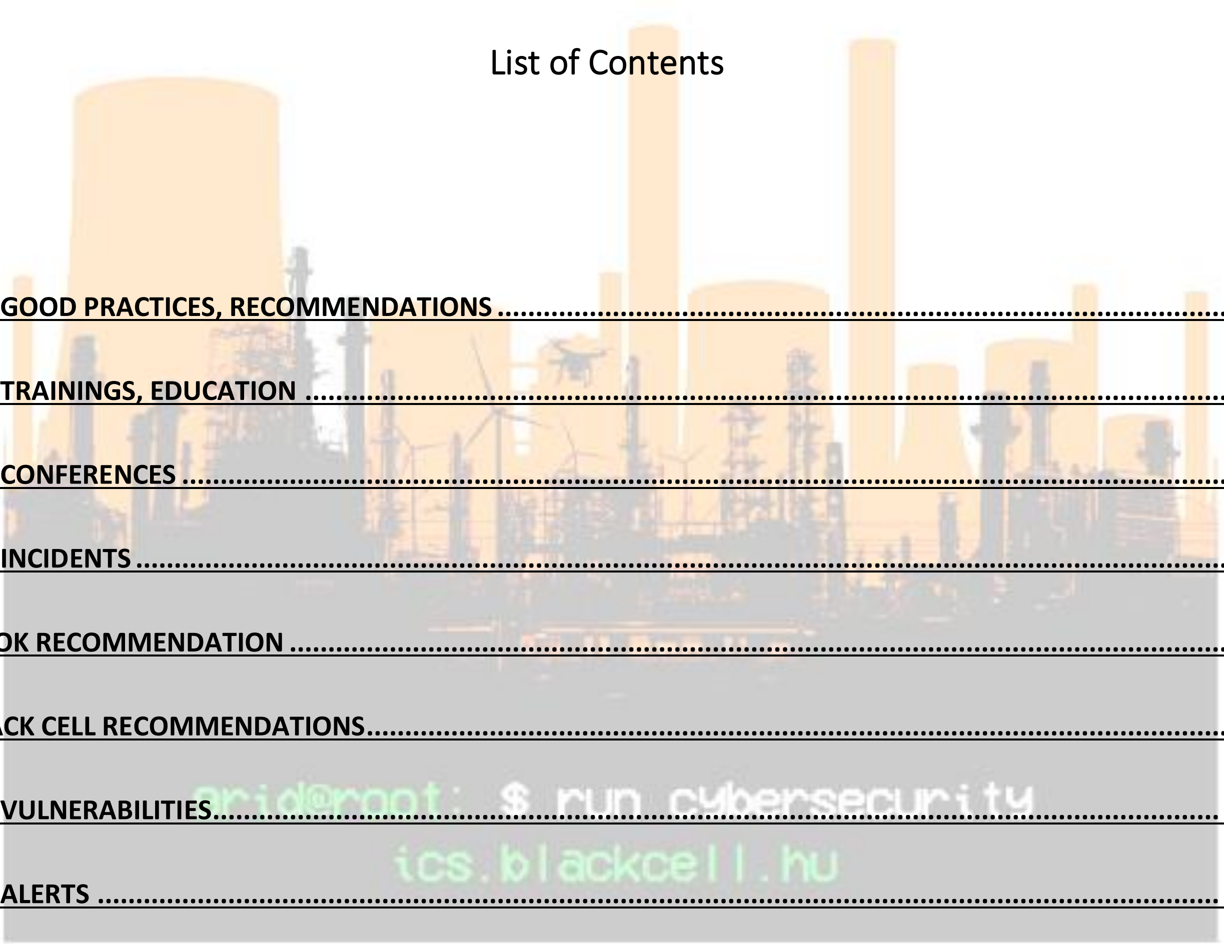
2021. March, Industrial Control Systems security feed

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



ICS GOOD PRACTICES, RECOMMENDATIONS 2

ICS TRAININGS, EDUCATION 3

ICS CONFERENCES 6

ICS INCIDENTS 7

BOOK RECOMMENDATION 8

BLACK CELL RECOMMENDATIONS........ 9

ICS VULNERABILITIES........ 10

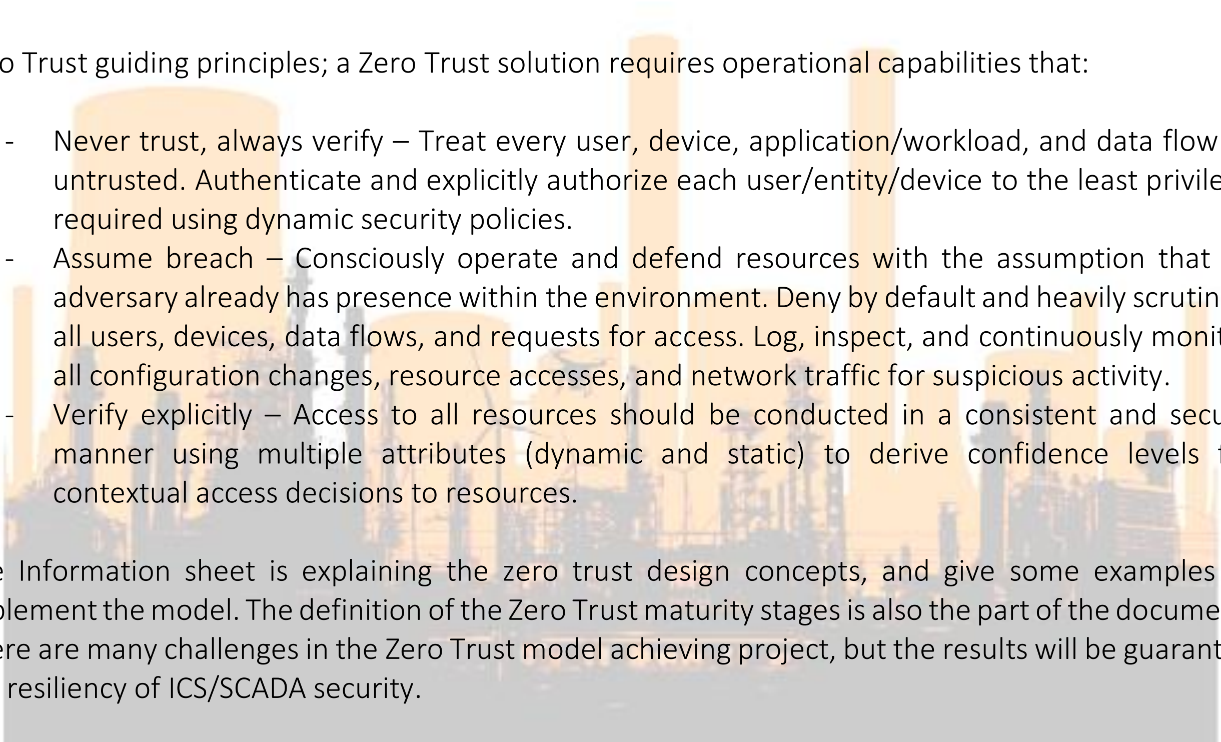
ICS ALERTS 15

ICS good practices, recommendations

NSA Releases Guidance on Zero Trust Security Model

The National Security Agency (NSA) has released Cybersecurity Information Sheet: Embracing a Zero Trust Security Model.

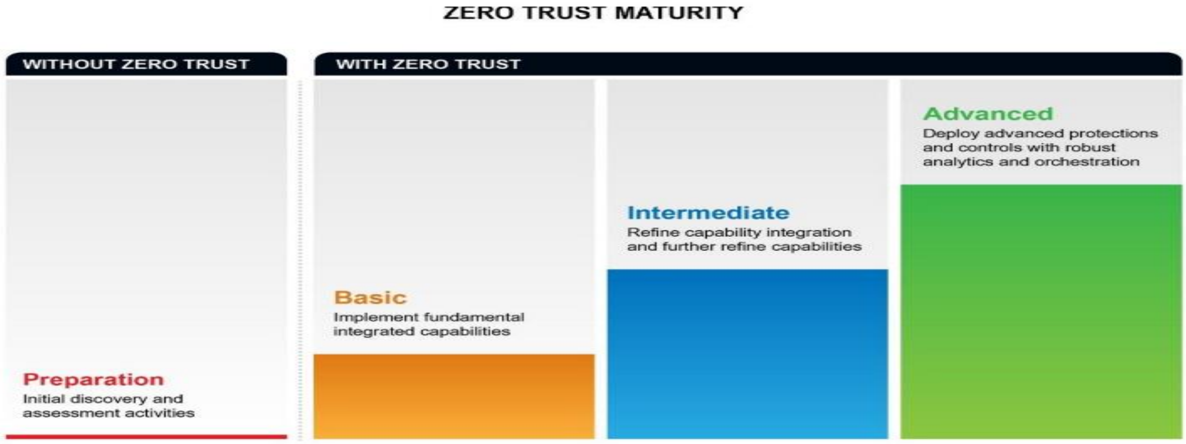
Nowadays, the Zero Trust model is a very important security solution in the ICS/SCADA environment. The number of insider threats and hacking activities growing every day. The Information sheet contains information about the increasingly sophisticated threats, describes how to achieve and what zero trust environment means.



Zero Trust guiding principles; a Zero Trust solution requires operational capabilities that:

- Never trust, always verify – Treat every user, device, application/workload, and data flow as untrusted. Authenticate and explicitly authorize each user/entity/device to the least privilege required using dynamic security policies.
- Assume breach – Consciously operate and defend resources with the assumption that an adversary already has presence within the environment. Deny by default and heavily scrutinize all users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity.
- Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources.

The Information sheet is explaining the zero trust design concepts, and give some examples to implement the model. The definition of the Zero Trust maturity stages is also the part of the document. There are many challenges in the Zero Trust model achieving project, but the results will be guarantee the resiliency of ICS/SCADA security.


ZERO TRUST MATURITY
WITHOUT ZERO TRUST
WITH ZERO TRUST
Advanced
Deploy advanced protections and controls with robust analytics and orchestration
Intermediate
Refine capability integration and further refine capabilities
Basic
Implement fundamental integrated capabilities
Preparation
Initial discovery and assessment activities

The Information sheet is available on the following link:

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

ICS trainings, education

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

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 **(New!)**

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
  - 26-01. April - May 2021.
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 19-23. April 2021.
  - 26-01. April - May 2021.
  - 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.

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:

- 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 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/

ICS conferences

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

ICS Cyber Security Conference

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.

Fairmont Singapore, Singapore; 27-29. April 2021.

More details can be found on the following website:

https://10times.com/ics-cyber-security-conference-singapore

ICS incidents

Chinese Hackers Targeted India's Power Grid

This hacking activity looks like a piece of hybrid warfare. The geopolitical situation is very tense in the region between Indian and Chinese borders.

Chinese hackers targeted India's Power Grid according to the news. This is an attack against a critical infrastructure, affected 12 organizations, 10 of which are in the power generation and transmission sector. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis.

Black Cell’s 2021. ICS security feed mentioned an incident with major power outage in India, this was a part of this coordinated activity probably from China. Security analysts said, that the attacker was APT41 (aka Barium, Winnti, or Wicked Panda).

Recorded Future said the attacks from China involved the use of infrastructure IT tracks as AXIOMATICASYMPTOTE, which encompasses a modular Windows backdoor called ShadowPad. There’s no exact information about the length of the power outage, except one statement: “It took two hours for the power supply to resume for essential services, prompting Chief Minister Uddhav Thackeray to order an enquiry into the incident.” but the seriousness of the activity is identified.

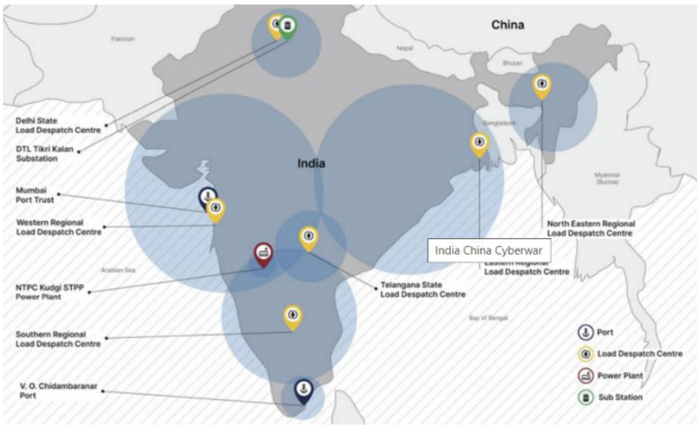
The incident was reported to the relevant CERT, but the incident handling process hasn’t been finished yet. This big volume attack is more complicated, and need to identify all of the relations to solve the problem.

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

https://theopensecurity.com/article/112-chinese-hackers-targeted-india-s-power-grid-amid-geopolitical-tensions/

https://thehackernews.com/2021/03/chinese-hackers-targeted-indias-power.html *

https://indianexpress.com/article/world/border-tension-chinese-hackers-indias-power-malware-us-firm-7209579/


China
Pakistan
Nepal
Bhutan
Bangladesh
India
Myanmar (Burma)
Arabian Sea
Bay of Bengal
Delhi State Load Despatch Centre
DTL Tikri Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
NTPC Kudgi STPP Power Plant
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port
Telangana State Load Despatch Centre
Eastern Regional Load Despatch Centre
North Eastern Regional Load Despatch Centre
India China Cyberwar
Port
Load Despatch Centre
Power Plant
Sub Station

*Source

Book recommendation

Hacking SCADA/Industrial Control Systems: The Pentest Guide

This book, published in 2016 is discussing why hackers attacking the industrial controls systems and especially SCADA systems. The first chapter presents some case studies from 2013-2014, and contains the ICS-CERT report from 2015.

The author presents the fourth-generation architecture of the SCADA systems.

1. Monolithic
2. Distributed
3. Networked
4. Internet of Things

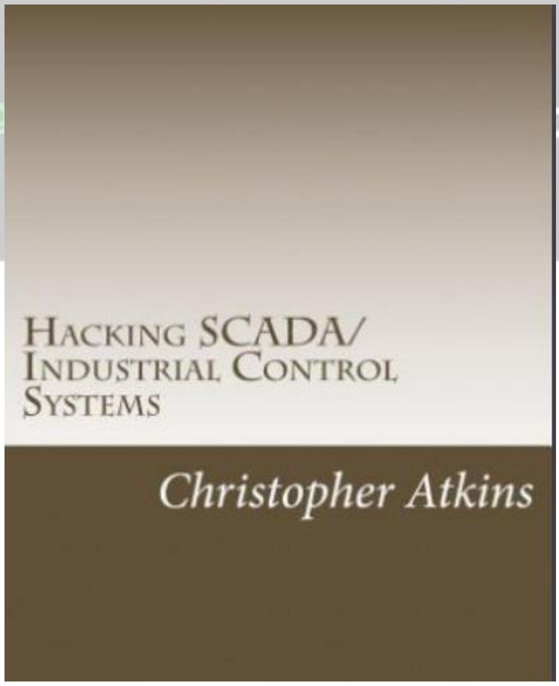
After the architecture review the network security tests and the user interface testing presented. The ICS protocol evaluation and the field devices also presented in the book, with many analysis methodologies and connected things. This is a very useful book for ICS/SCADA pentesters.

Authors/Editors: Christopher Atkins

Year of issue: 2016.

The book available at the following link:

https://www.libristo.hu/hu/konyv/hacking-scada-industrial-control-systems-the-pentest-guide_17665167?utm_source=google&utm_medium=surfaces&utm_campaign=shopping%20feed&utm_content=free%20google%20shopping%20clicks%20merchant_hu&gclid=EAIaIQobChMI4cL1-Yz97gIVSkeRBR3oRQBwEAYYCCABEgLfnfD_BwE



Black Cell recommendations

Industrial Control System Community of Interest

There are many associations around the world in case of industrial control systems security. One of them is the ICS COI, a UK community.

Cyber Security experts say that information sharing is very important, but in most cases, details are missing. Many organizations want to join these associations and got some very useful information from the group. Unfortunately, many of them doesn't want to give information. This is a problem in a cooperation.

The cooperation will be successful if the members have a framework with defined tasks. ICS operators, asset owners, security researchers, vendors, regulators, integrators and academists must have clearly defined tasks to help to each other.

ICS COI in the UK established association with the following benefits:

- The opportunity to share knowledge, expertise, and experience within a trusted ICS security community.
- Building and maintaining ICS security and safety-related expertise within the UK.
- Identifying new and emerging ICS security requirements.
- The opportunity to work on complex, cross sector ICS issues generated by the ICS COI Steering Group.

By collaborating based on an elaborated framework, an ICS security community can help to the stakeholders to enhance security. There is many information, which is very important to the ICS operators and the sources of information are security researchers.

The earlier was just one example, but there are further benefits, if the community finds all of the important types of information and the platform to share with the others.

It's recommended to find a community with relevant organizations. If the details are clear, the community will be effective and helpful for the members.

The related article is available at the following link:

https://www.ncsc.gov.uk/blog-post/strength-of-ics-coi-is-the-team

ICS vulnerabilities

In March 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:

ICSMA-21-084-01: Philips Gemini PET/CT Family
Law level vulnerability: Storage of Sensitive Data in a Mechanism Without Access Control.
https://us-cert.cisa.gov/ics/advisories/icsma-21-084-01

ICSA-21-082-01: Weintek EasyWeb cMT
Critical level vulnerabilities: Code Injection, Improper Access Control, Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-082-01

ICSA-21-082-02: GE MU320E
Critical level vulnerabilities: Use of Hard-coded Password, Execution with Unnecessary Privileges, Inadequate Encryption Strength.
https://us-cert.cisa.gov/ics/advisories/icsa-21-082-02

ICSA-21-082-03: GE Reason DR60
Critical level vulnerabilities: Hard-coded Password, Code Injection, Execution with Unnecessary Privileges.
https://us-cert.cisa.gov/ics/advisories/icsa-21-082-03

ICSA-21-054-04: Ovarro TBox
High level vulnerabilities: Code Injection, Incorrect Permission Assignment for Critical Resource, Uncontrolled Resource Consumption, Insufficiently Protected Credentials, Use of Hard-coded Cryptographic Key.
https://us-cert.cisa.gov/ics/advisories/icsa-21-054-04

ICSA-21-061-02: Rockwell Automation CompactLogix 5370 and ControlLogix 5570 Controllers (Update A) Medium level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-061-02

ICSA-21-033-01: Rockwell Automation MicroLogix 1400 (Update A)
High level vulnerability: Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-033-01

ICSA-21-077-01: Johnson Controls Exacq Technologies exacqVision
Medium level vulnerability: Information Exposure.
https://us-cert.cisa.gov/ics/advisories/icsa-21-077-01

ICSA-21-077-02: Hitachi ABB Power Grids eSOMS
High level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-21-077-02

ICSA-21-077-03: Hitachi ABB Power Grids eSOMS Telerik

Critical level vulnerabilities: Path Traversal, Deserialization of Untrusted Data, Improper Input Validation, Inadequate Encryption Strength, Insufficiently Protected Credentials, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-077-03

ICSA-21-056-03: **Rockwell Automation Logix Controllers (Update A)**
Critical level vulnerability: Insufficiently Protected Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-056-03

ICSA-21-075-01: **Advantech WebAccess/SCADA**
Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-075-01

ICSA-21-075-02: **GE UR family**
Critical level vulnerabilities: Inadequate Encryption Strength, Session Fixation, Exposure of Sensitive Information to an Unauthorized Actor, Improper Input Validation, Unrestricted Upload of File with Dangerous Type, Insecure Default Variable Initialization, Use of Hard-coded Credentials.
https://us-cert.cisa.gov/ics/advisories/icsa-21-075-02

ICSA-21-075-03: **Hitachi ABB Power Grids AFS Series**
Medium level vulnerability: Infinite Loop.
https://us-cert.cisa.gov/ics/advisories/icsa-21-075-03

ICSMA-17-017-02: **BD Alaris 8015 PC Unit (Update B)**
Medium level vulnerabilities: Insufficiently Protected Credentials, Security Features.
https://us-cert.cisa.gov/ics/advisories/icsma-17-017-02

ICSA-21-070-01: **Schneider Electric IGSS SCADA Software**
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://us-cert.cisa.gov/ics/advisories/icsa-21-070-01

ICSA-21-068-01: **Siemens SIMATIC S7-PLCSIM**
Medium level vulnerabilities: Infinite Loop, NULL Pointer Dereference, Divide by Zero.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-01

ICSA-21-068-02: **Siemens SCALANCE and RUGGEDCOM Devices SSH**
High level vulnerability: Improper Restriction of Excessive Authentication Attempts.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-02

ICSA-21-068-03: **Siemens SCALANCE and RUGGEDCOM Devices**
High level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-03

ICSA-21-068-04: **Siemens SINEMA Remote Connect Server**
High level vulnerability: Incorrect Authorization.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-04

ICSA-21-068-05: **Siemens LOGO! 8 BM**

Medium level vulnerability: Improper Handling of Exceptional Conditions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-05

ICSA-21-068-06: **TCP/IP Stack Vulnerabilities–AMNESIA:33 in SENTRON PAC / 3VA Devices**

Medium level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-06

ICSA-21-068-07: **Siemens TCP Stack of SIMATIC MV400**

High level vulnerabilities: Improper Validation of Specified Index, Position, or Offset in Input; Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-07

ICSA-21-068-08: **Siemens Energy PLUSCONTROL 1st Gen**

Medium level vulnerability: Predictable Exact Value from Previous Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-08

ICSA-21-068-09: **Siemens Solid Edge File Parsing**

High level vulnerabilities: Out-of-bounds Write, Improper Restriction of XML External Entity Reference, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-09

ICSA-21-068-10: **Siemens SCALANCE and SIMATIC libcurl**

High level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-10

ICSA-21-035-01: **Luxion KeyShot** (Update A)

High level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Insufficient UI Warning of Dangerous Operations, Untrusted Pointer Dereference, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-035-01

ICSA-21-019-01: **dnsmasq by Simon Kelley** (Update A)

High level vulnerabilities: Heap-based Buffer Overflow, Insufficient Verification of Data Authenticity, Use of a Broken or Risky Cryptographic Algorithm.
https://us-cert.cisa.gov/ics/advisories/icsa-21-019-01

ICSA-20-343-05: **Siemens Embedded TCP/IP Stack Vulnerabilities–AMNESIA:33** (Update B)

Medium level vulnerability: Integer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

ICSA-20-196-05: **Siemens UMC Stack** (Update F)

Medium level vulnerabilities: Unquoted Search Path or Element, Uncontrolled Resource Consumption, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-161-04: **Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK** (Update F)

Medium level vulnerability: Unquoted Search Path or Element.

https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04

ICSA-20-105-08: **Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update B)**

High level vulnerability: Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-20-105-08

ICSA-20-042-04: **Siemens PROFINET-IO Stack (Update D)**

High level vulnerability: Uncontrolled Resource Consumption.

https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04

ICSA-19-162-02: **Siemens SIMATIC Ident MV440 Family (Update A)**

High level vulnerabilities: Improper Privilege Management, Cleartext Transmission of Sensitive Information.

https://us-cert.cisa.gov/ics/advisories/ICSA-19-162-02

ICSA-19-099-04: **Siemens SINEMA Remote Connect (Update A)**

High level vulnerabilities: Incorrect Calculation of Buffer Size, Out-of-bounds Read, Stack-based Buffer Overflow, Improper Handling of Insufficient Permissions.

https://us-cert.cisa.gov/ics/advisories/ICSA-19-099-04

ICSA-17-339-01: **Siemens Industrial Products (Update Q)**

High level vulnerability: Improper Input Validation.

https://us-cert.cisa.gov/ics/advisories/ICSA-17-339-01

ICSA-17-129-02: **Siemens PROFINET DCP (Update S)**

Medium level vulnerability: Improper Input Validation.

https://us-cert.cisa.gov/ics/advisories/ICSA-17-129-02

ICSA-21-063-01: **Rockwell Automation 1734-AENTR Series B and Series C**

High level vulnerabilities: Improper Access Control, Cross-site Scripting.

https://us-cert.cisa.gov/ics/advisories/icsa-21-063-01

ICSA-21-063-02: **Schneider Electric EcoStruxure Building Operation (EBO)**

Medium level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Cross-site Scripting, Improper Restriction of XML External Entity Reference, Improper Access Control, Windows Unquoted Search Path.

https://us-cert.cisa.gov/ics/advisories/icsa-21-063-02

ICSA-21-061-01: **Hitachi ABB Power Grids Ellipse EAM**

Medium level vulnerabilities: Cross-site Scripting, User Interface Misrepresentation of Critical Information.

https://us-cert.cisa.gov/ics/advisories/icsa-21-061-01

ICSA-21-061-02: **Rockwell Automation CompactLogix 5370 and ControlLogix 5570 Controllers**

Medium level vulnerability: Improper Input Validation.

https://us-cert.cisa.gov/ics/advisories/icsa-21-061-02

ICSA-21-061-03: MB connect line mbCONNECT24, mymbCONNECT24

High level vulnerabilities: Improper Privilege Management, Server-side Request Forgery (SSRF), Cross-site Scripting, Uncontrolled Resource Consumption, Open Redirect, Insecure Default Initialization of Resource, PHP Remote File Inclusion, Use of Hard-coded Credentials, Exposure of Sensitive Information to an Unauthorized Actor, Files or Directories Accessible to External Parties.
https://us-cert.cisa.gov/ics/advisories/icsa-21-061-03

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 March 2021, ICS-CERT hasn’t published alerts.

The previous alerts can be found at the following link:

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