2022. February, 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

5 Ways to Reduce the Risk of Ransomware to Your OT Network

In the last few months there were at least three hight impact ransomware attacks against industrial stakeholders. Even though none of these attacks appear to have impacted the OT environment directly, they had significant impact on the OT systems lead to catastrophic shutdowns. Ransomware attacks are disrupting pipelines, processing plants, and food distribution. These are one of the many main pillars of the supply of modern society.

These attacks could happen in any time at any sector as experts estimated that a ransomware attack will occur every 11 seconds in 2021. The average downtime a company experiences after a ransomware attack is 21 days. To imagine the possible negative effects of a downtime like this, just think about if a hospital (critical infrastructure) goes down for 21 days. To avoid these high impact attacks, the OT systems should be hardened.

To properly harden the OT infrastructure and to reduce the risk of a ransomware attack here are 5 recommendation:

1. Extend the scope of your risk governance to include anything that is a cyber-physical asset
   We must know what our company has. Even if it's an IT, OT or an IoT asset every of these has a few weak spots. To mitigate most of the vulnerabilities first thing for every organization is to assess all of the assets they have and fit the scope to every vulnerable asset they have.

2. Make sure that you have proper segmentation between IT and OT networks.
   These ransomware attacks are not aiming for the ICS/OT of the company but for the IT. All of the organizations who work with OT systems have to properly separate the IT and the OT systems. The segmentation can be done via firewall rules and settings and by virtual segmentation to zones within the OT environment. Also, if it's an option do not let the direct remote operations of the OT systems. If remote operations need direct access into the OT networks, make sure this is done through a secure remote access connection with strict controls over users, devices, and sessions.

3. Practice good cyber hygiene. Ensure that your hygiene extends to OT and IoT devices
   The weakest link is the human factor. The most important thing is the awareness. If the users create strong passwords, don't reuse them and they use multifactor authentication most of the human factors are mitigated. It is hard to create and force these rules on some of the legacy systems. If it's not possible due to the technical limitations of the legacy system you must find another solution to mitigate those threats such as virtualization, firewall rules, DMZs, etc.

4. Implement a robust system monitoring program.
   To mitigate threats, you must first see those coming. Without a proper monitoring system the malicious activities cannot be seen and there is no way to react on time to avoid the consequences. Continuous threat monitoring across the OT network can be implemented quickly, integrate equally well with OT and IT systems and workflows, and allow IT and OT teams to look at OT environments together.

5. Run exercises on your incident response plan.
   To prepare for the ransomware attacks your company must create tabletop exercises and regularly practise those. These can help you to understand the risks and a good opportunity to improve the incident response capability.

By taking a few simple, foundational steps you can reduce the risk of ransomware to your industrial environments.

Source and more information are available on the following link:

https://www.securityweek.com/5-ways-reduce-risk-ransomware-your-ot-network

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in March 2022:

O'Reilly provides a 10-day free trial training course. In this Industrial Cybersecurity training you get O'Reilly members experience live online training, plus books, videos, and digital content from 200+ publishers.

More details can be found on the following website:

https://www.oreilly.com/library/view/industrial-cybersecurity/9781788395151/60f43e9e-1d7b-4fe8-89de-87b70052da85.xhtml

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:

- 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
  - 21-26. March 2022
  - 26-31. March 2022
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - 07-12. March 2022
  - 21-26. March 2022
  - 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)

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.

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/

New course and seminar in the ICS security feed:

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

SCADA CYBER SECURITY: Your Firewall/VPN is Not Enough

Critical infrastructure that impacts our daily lives relies on remote IP-connected SCADA equipment - and hackers know it. Multitudes of inexpensive and widespread SCADA sensors and controls remain totally unprotected due merely to the logistical difficulty of reaching them all. Some SCADA installations are protected by traditional firewalls, but this protection extends the corporate network to the remote site, thereby increasing the attack surface and the motivation for hacking. This is not just a potential cyber security nightmare; attacks occur constantly. This talk will discuss these threats and explain how to prevent them, while also protecting the corporate network from intrusion.

Las Vegas, NV; 22nd March, 2022

More details can be found on the following website:

https://agenda.iwceexpo.com/session/scada-cyber-security-your-firewallvpn-is-not-enough/884816

Cyber Security for Manufacturing Summit

#ManuSec Europe is an intimate and exclusive platform for IT and OT security leaders from Europe's manufacturing industry to exchange in-depth cyber security knowledge. Senior cyber security professionals share first-hand insights through real-life case studies, panel debates, and keynote presentations, while bringing forth questions and challenges to be discussed over roundtables and dynamic networking breaks.

This is your annual opportunity to stay engaged with the manufacturing cyber security community, build cross-departmental cyber security partnerships, benchmark your company's digital maturity against peers, maintain competitive edge and participate in the discussions shaping European manufacturers' cyber security strategies in 2022 and beyond.

Munich, Germany; 22nd – 23rd March 2022

More details can be found on the following website:

https://europe.manusecevent.com/

CCISCS 2022: 16. International Conference on Cybersecurity for 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 Cybersecurity for 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 Cybersecurity for 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 Cybersecurity for Industrial Control Systems.

Singapore, Singapore; March 28th -29th, 2022

More details can be found on the following website:

https://waset.org/cybersecurity-for-industrial-control-systems-conference-in-march-2022-in-singapore

ICS incidents

German oil companies hit by ransomware attack

The end of January, a ransomware hit German oil companies in Northern Germany. The cyberattack affected 233 gas stations, where the automatic systems failed, and the companies had to operate the processes manually because of the incident.

After the detection, the Oiltanking GmbH activated the continuity plans to solve the disruption. The most affected system was which was responsible for the automation of tank loading and unloading processes. In total, dozens of terminals with oil storage and transport around the world had been affected, with firms reporting that the attacks occurred over this weekend.

Oiltanking Deutschland GmbH & Co. KG terminals were operated with limited capacity and it declared force majeure.

The 13 tank farms that Oiltanking operates cannot currently serve trucks, so the firm has turned to alternative methods. The economic impact of cyberattacks affecting the greater supply chain can prove to be extremely detrimental.

Source: https://www.bbc.com/news/technology-60250956

The source and more information available on the following links:

https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/
https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack

Book recommendation

Techno Security's Guide to Securing SCADA: A Comprehensive Handbook On Protecting The Critical Infrastructure 1st Edition

Around the world, SCADA (supervisory control and data acquisition) systems and other real-time process control networks run mission-critical infrastructure--everything from the power grid to water treatment, chemical manufacturing to transportation. These networks are at increasing risk due to the move from proprietary systems to more standard platforms and protocols and the interconnection to other networks. Because there has been limited attention paid to security, these systems are seen as largely unsecured and very vulnerable to attack.

This book addresses currently undocumented security issues affecting SCADA systems and overall critical infrastructure protection. The respective co-authors are among the leading experts in the world capable of addressing these related-but-independent concerns of SCADA security. Headline-making threats and countermeasures like malware, sidejacking, biometric applications, emergency communications, security awareness planning, personnel & workplace preparedness and bomb threat planning will be addressed in detail in this one-of-a-kind book-of-books dealing with the threats to critical infrastructure protection.

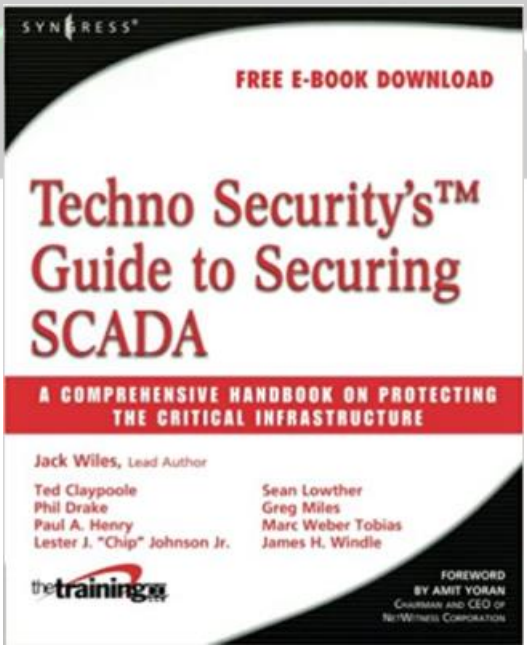
The book was written in 2008 but still contains current problems and challenges in SCADA protection.

Authors/Editors: Jack Wiles.

Year of issue: 2008

The book is available at the following link:

https://www.sciencedirect.com/book/9781597492829/techno-securitys-guide-to-securing-scada#book-info



Black Cell recommendations

Cyber Assessment Methods for SCADA Security

The SCADAhacker website collects many useful links, documents, vulnerabilities, exploits, frameworks, maturity models and other ICS/SCADA security related things. There are some good practices on the website, one of them is the Cyber Assessment Methods for SCADA Security.

The SCADA security assessment is very important to know, as this assessment can tell how effective and comprehensive the organization's security regarding OT devices.

The following resources and advices are valuable in the assessment process:

- Dedicated semi-private work area
- Broadband (reliable) internet access for research
- Vendor help and support
- Backing up the target (SCADA) system
- Reboot the system after every attack to ensure all of the effects are presented; some effects may not be apparent until it has been rebooted.
- Prioritize vulnerabilities based on their probability of exploitation and the damages their exploitation would cause

First, you must determine the assessment methodology. After that it is very important to test the environment configuration. If the test is effective, you could find the vulnerabilities and assess them.

The document contains many useful tools to help execute the assessment, for example, NMAP, NESSUS, STAT Scanner, Ethereal etc.

Reporting is also very important. The details of the reports and content is critical, because if the findings and details are not clear, the mitigation wouldn't be effective.

This document is strongly recommended to apply for the SCADA operators if they want to know the SCADA systems' weak points and correct them.

Source and more details available on the following link:

https://scadahacker.com/library/Documents/Assessment_Guidance/ISA%20-%20Paper%20-%20Cyber%20Assessments%20Methods%20for%20SCADA.pdf

ICS vulnerabilities

In February 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-22-055-01: **FATEK Automation FvDesigner**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-055-01

ICSA-22-055-02: **Mitsubishi Electric EcoWebServerIII**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation, Uncontrolled Resource Consumption, Improperly Controlled Modification of Dynamically-Determined Object Attributes.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-055-02

ICSA-22-055-03: **Schneider Electric Easergy P5 and P3**

High level vulnerabilities: Use of Hard-coded Credentials, Classic Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-055-03

ICSA-21-231-02: **Baker Hughes Bently Nevada 3500**

High level vulnerability: Use of Password Hash with Insufficient Computational Effort.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-231-02

ICSA-22-053-01: **GE Proficy CIMPLICITY-IPM**

High level vulnerability: Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-053-01

ICSA-22-053-02: **GE Proficy CIMPLICITY-Cleartext**

High level vulnerability: Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-053-02

ICSA-22-053-03: **WIN-911 2021**

Medium level vulnerability: Incorrect Default Permissions.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-053-03

ICSA-22-046-01: **Schneider Electric IGSS**

Critical level vulnerabilities: Integer Overflow or Wraparound, Path Traversal, Classic Buffer Overflow, Out-of-bounds Read, Improper Initialization, Missing Authorization.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-046-01

ICSA-22-041-01: **Siemens SIMATIC Industrial Products**

High level vulnerabilities: Operation on a Resource after Expiration or Release, Missing Release of Memory after Effective Lifetime.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-01

ICSA-22-041-02: **Siemens SIMATIC WinCC and PCS**

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-22-041-03: Siemens Simcenter Femap
High level vulnerabilities: Out-of-bounds Write, Access of Resource Using Incompatible Type, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-03

ICSA-22-041-04: SINEMA Remote Connect Server
Medium level vulnerability: Open Redirect.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-04

ICSA-22-041-05: SICAM TOOLBOX II
Critical level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-05

ICSA-22-041-06: Siemens Spectrum Power 4
Medium level vulnerability: Cross-site scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-06

ICSA-22-041-07: Siemens Solid Edge, JT2Go, and Teamcenter Visualization
High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-07-1

ICSA-22-041-01: Siemens SIMATIC Industrial Products
High level vulnerabilities: Operation on a Resource after Expiration or Release, Missing Release of Memory after Effective Lifetime.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-01

ICSA-22-041-02: Siemens SIMATIC WinCC and PCS
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-22-041-03: Siemens Simcenter Femap
High level vulnerabilities: Out-of-bounds Write, Access of Resource Using Incompatible Type, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-03

ICSA-22-041-04: SINEMA Remote Connect Server
Medium level vulnerability: Open Redirect.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-04

ICSA-22-041-05: SICAM TOOLBOX II
Critical level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-05

ICSA-22-041-06: Siemens Spectrum Power 4
Medium level vulnerability: Cross-site scripting.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-06

ICSA-22-013-05: Siemens COMOS Web (Update A)
High level vulnerabilities: Basic XSS, Relative Path Traversal, SQL Injection, Cross-site Request Forgery.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-013-05

ICSA-21-350-16: Siemens Healthineers syngo fastView (Update A)
High level vulnerabilities: Out-of-bounds Write, Write-what-where Condition.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-350-16

ICSA-21-315-03: Siemens SIMATIC WinCC (Update A)
Critical level vulnerabilities: Path Traversal, Insertion of Sensitive Information into Log File.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-03

ICSA-21-257-13: Siemens LOGO! CMR and SIMATIC RTU 3000 (Update A)
Medium level vulnerability: Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-257-13

ICSA-21-222-05: Siemens Industrial Products Intel CPUs (Update A)
High level vulnerability: Missing Encryption of Sensitive Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-05

ICSA-21-068-06: Siemens TCP/IP Stack Vulnerabilities–AMNESIA:33 in SENTRON PAC / 3VA Devices (Update C)
Medium level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-068-06

ICSA-20-105-07: Siemens SCALANCE & SIMATIC (Update F)
High level vulnerability: Resource Exhaustion.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-105-07

ICSA-20-042-02: Siemens Industrial Products SNMP (Update E)
High level vulnerabilities: Data Processing Errors, NULL Pointer Dereference.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-042-02

ICSA-20-014-03: Siemens SCALANCE X Switches (Update A)
High level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-014-03

ICSA-19-225-03: Siemens SCALANCE X Switches (Update D)

High level vulnerability: Insufficient Resource Pool.
https://www.cisa.gov/uscert/ics/advisories/icsa-19-225-03

ICSA-22-041-07: Siemens Solid Edge, JT2Go, and Teamcenter Visualization
High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-bounds Read.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-07-0

ICSA-17-129-02: Siemens PROFINET DCP (Update V)
Medium level vulnerability: Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/ICSA-17-129-02

ICSA-21-049-02: Mitsubishi Electric FA Engineering Software Products (Update D)
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 F)
High level vulnerability: Unquoted Search Path or Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-212-04

ICSA-22-034-01: Sensormatic PowerManage
Critical level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-034-01

ICSA-22-034-02: Airspan Networks Mimosa
Critical level vulnerabilities: Improper Authorization, Incorrect Authorization, Server-side Request Forgery, SQL Injection, Deserialization of Untrusted Data, OS Command Injection, Use of a Broken or Risky Cryptographic Algorithm.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-034-02

ICSA-21-243-02: FANUC Robot Controllers (Update A)
High level vulnerabilities: Integer Coercion Error, Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-243-02

ICSA-22-032-01: Ricon Mobile Industrial Cellular Router
Critical level vulnerability: OS Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-01

ICSA-22-032-02: Advantech ADAM-3600
Critical level vulnerability: Use of Hard-coded Cryptographic Key.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-032-02

ICSA-21-315-02: Multiple Data Distribution Service (DDS) Implementations (Update A)
High level vulnerabilities: Write-what-where Condition, Improper Handling of Syntactically Invalid Structure, Network Amplification, Incorrect Calculation of Buffer Size, Heap-based Buffer

Overflow, Improper Handling of Length Parameter Inconsistency, Amplification, Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-02

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 February 2022, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

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