2023 April, 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

ENISA Transport Threat Landscape

ENISA published an analysis which described the threat landscape of the Transport sector.

This is the first analysis conducted by the European Union Agency for Cybersecurity (ENISA) of the cyber threat landscape of the transport sector in the EU. The report aims to bring new insights into the reality of the transport sector by mapping and studying cyber incidents from January 2021 to October 2022. It identifies prime threats, actors and trends based on the analysis of cyberattacks targeting aviation, maritime, railway and road transport over a period of almost 2 years.

During the reporting period, the threat actors with the biggest impact on the sector were state-sponsored actors, cybercriminals and hacktivists. ENISA observed the following trends (not complete):

- The majority of attacks on the transport sector target information technology (IT) systems. Operational disruptions can occur as a consequence of these attacks, but the operational technology (OT) systems are rarely being targeted.
- Ransomware groups will likely target and disrupt OT operations in the foreseeable future.

The report also highlights issues with the reporting of cyber incidents and the fact that we still have limited knowledge and information regarding such incidents. The analysis in this report indicates that publicly disclosed incidents are just the tip of the iceberg.

We strongly recommend the transport sector operators to study the report.

Source and more information available on the following link:

https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in May 2023:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- 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

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

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

- Industrial Control System (ICS) & SCADA Cyber Security Training

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- ICS/SCADA security training seminar

https://www.enoinstitute.com/scada-ics-security-training-seminar/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

ICS conferences

In May 2023, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

SGF Cybersecurity Week 2023

This forum brings together utility CISOs with their IT and OT cybersecurity teams for an in-depth discussion around the impact of geopolitics on the evolving threat landscape, the emergence of new grid vulnerabilities in the context of increased grid innovation and interconnection, the latest IT and OT cybersecurity solutions on the market and in development, and the implications of multiple regulatory frameworks with competing demands underpinning cybersecurity strategies.

Amsterdam, Netherlands; 15th – 19th May 2023

More details can be found on the following website:

https://industrialcyber.co/event/sgf-cybersecurity-week-2023/

IoT Tech Expo North America 2023

Don’t miss the chance to explore how Internet of Things, Smart Infrastructures and Connectivity are having an impact on a range of industries, including: manufacturing, transport, supply chain, government, legal and finance sectors, energy, retail, healthcare and more!

Exploring the latest challenges, opportunities and innovations within the Internet of Things and covering the impact it has across industry sectors. Our community of industry experts will explore and debate the technological advancements across the IoT ecosystem and beyond.

Santa Clara Convention Center, California; 17th – 18th May 2023

More details can be found on the following website:

https://www.iottechexpo.com/northamerica/

The Digital Oil & Gas Summit 2023

As the oil and gas industry navigates the ever-changing digital transformation landscape, staying ahead of the curve is more important than ever.

The Digital Oil and Gas Summit brings together leaders in digital transformation, data analytics, cybersecurity, and more to share their insights and critical strategies for success in the digital age. From exploring the latest advances in artificial intelligence and machine learning to discuss best practices for managing data privacy and security you'll find all the answers you need in Lisbon this coming May!

Lisbon, Portugal; 24th – 25th May 2023

More details can be found on the following website:

https://oilandgas-iot.com/?ref=infosec-conferences.com

ICS incidents

Dole Experiences Cybersecurity Incident

Dole plc. announced in February that the company recently experienced a cybersecurity incident that has been identified as ransomware.

While details of the attack remain limited, the cyberattack did result in disruption to Dole's North American operations. Two grocery stores located in Texas and New Mexico contacted CNN, informing the news outlet of their inability to stock Dole's salad kits.

Major food producers are a part of the critical infrastructure ecosystem. Attacks like the one executed against Dole highlight vulnerabilities in this ecosystem and highlight the need to understand and manage cyber risk.

In its latest SEC filing, Dole reiterated that the "sophisticated ransomware attack" had limited impact on its operations.

The company said in a conference call earlier this month that it does not expect to recover losses caused by the ransomware attack through cyberinsurance or supplier recovery.

It's unclear which ransomware group was behind the attack. SecurityWeek has checked the leak sites of several major operations and found no mention of Dole at the time of writing.

The cybercrime group that conducted the attack may not have a leak website, but it's also possible that Dole decided to pay the ransom demanded by the hackers.

The sources are available on the following links:

https://www.doleplc.com/news/company-news/company-news-details/2023/-Dole-Experiences-Cybersecurity-Incident/default.aspx

https://www.informationweek.com/security-and-risk-strategy/looking-at-the-dole-cyberattack-and-the-future-of-critical-infrastructure-cybersecurity-

https://www.securityweek.com/dole-says-employee-information-compromised-in-ransomware-attack/

Book recommendation

Physical and Cyber Safety in Critical Water Infrastructure

Water supply and water management services are among the most critical infrastructures in society, providing safe and affordable drinking water, managing wastewater to avoid floods and environmental pollution, and enabling the reuse and replenishment of scarce water resources. With water and wastewater facilities and infrastructure intrinsic to our towns and cities, we must not underestimate the potentially catastrophic results of water supply contamination or disruption to the systems that regulate the water we rely on for essential agricultural, environmental, and municipal needs.

This book presents 12 papers selected from those delivered at the NATO Advanced Research Workshop (ARW) on Physical and Cyber Safety in Critical Water Infrastructure, held in Oslo, Norway, from 8-11 October 2018. The conference brought together resource persons and decision makers from 12 NATO countries and 6 partner countries to share their experiences with the objective of formulating best practice based on recommendations and conclusions, to increase awareness of the risks that threaten current and future water utilities and services, to learn how to improve surveillance and preparedness, and to deal with a crisis should all else fail.

Addressing the urgent need to focus on physical and cyber safety in one of the most critical infrastructures in our society, the book will be of interest to all those working in the field of water supply and waste water management.

Authors/Editors: Ratnaweera, H., Pivovarov, O.A. (Editors)

Year of issue: 2019

The book is available at the following link:

https://www.iospress.com/catalog/books/physical-and-cyber-safety-in-critical-water-infrastructure

NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 56

Physical and Cyber
Safety in Critical Water
Infrastructure

Edited by
Harsha Ratnaweera
Oleksandr A. Pivovarov

IOS
Press

NATO
OTAN

This publication is supported by

The NATO Science for Peace and Security Programme

ICS security news selection

Leaked Documents Detail Russia's Cyberwarfare Tools, Including for OT Attacks

Documents leaked from Russian IT contractor NTC Vulkan show the company's possible involvement in the development of offensive hacking tools, including for the advanced persistent threat (APT) actor known as Sandworm, Mandiant reports.

Based in Moscow, NTC Vulkan advertises its collaboration with Russian organizations and government agencies, without mentioning any involvement in the operations of state-sponsored groups or intelligence services.

Documents dated between 2016 and 2020, however, show that the company has been contracted by Russian intelligence, including the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) Unit 74455 (also known as Sandworm, Telebots, Iron Viking and Voodoo Bear), for the development of tools, training programs, and an intrusion platform. …

Source, and more information:

https://www.securityweek.com/leaked-documents-detail-russias-cyberwarfare-tools-including-for-ot-attacks/

Industrial Defender launches Phoenix to secure SMBs operations

Industrial Defender has unveiled the launch of Phoenix, an OT security solution tailored to the needs of SMBs.

Phoenix is revolutionizing how smaller industrial organizations approach OT security by providing visibility into all their OT assets and their associated cyber risks. By providing a solution that is easy to deploy and cost-effective, Phoenix enables SMBs to overcome resource barriers and secure their operations effectively.

"From ransomware campaigns to nation-state attacks, cyber threats against industrial organizations have never been higher. Attackers are increasingly targeting operational technology, and smaller organizations are especially vulnerable due to their limited resources," said Jay Williams, CEO of Industrial Defender. …

Source, and more information:

https://www.helpnetsecurity.com/2023/04/06/industrial-defender-phoenix/

Sekoia expects hackers to continue targeting energy sector through ransomware, hack-and-leak attacks

Data released by Sekoia disclosed that the energy sector was at the center of concern in Europe in 2022, particularly in light of the Russo-Ukrainian conflict. The sector was targeted by various offensive cyber-enabled operations, including espionage, disruption, sabotage, and information operations. Additionally, the European energy sector also faced lucrative-oriented cyber malicious campaigns, mostly double extortion attacks operated by Ransomware-as-a-Service (RaaS) groups, and hack-and-leak operations.

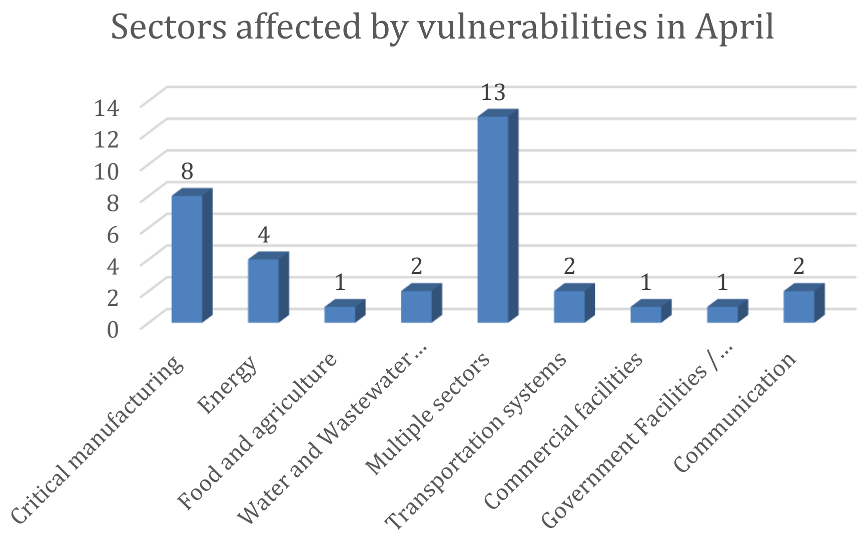
The energy sector remains particularly vulnerable to cyber threats, notably due to two identified structural risks being the complexity of information systems implemented in this sector, including IT and OT (operational technology) networks and solutions, in a context of digitization of activities and IT/OT convergence, as well as third party risk, both increasing the exposure to threat, with possible effects on the physical layer.

Source, and more information:

https://industrialcyber.co/utilities-energy-power-water-waste/sekoia-expects-hackers-to-continue-targeting-energy-sector-through-ransomware-hack-and-leak-attacks/

ICS vulnerabilities

In April 2023, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

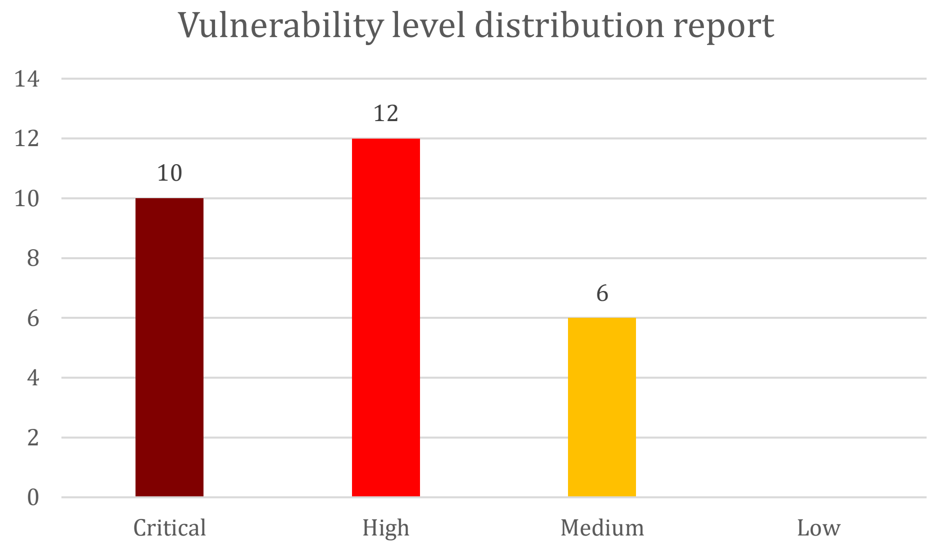


Average number of vulnerabilities per vulnerability report in April: **1,68**

Vulnerabilities/Exploitable remotely: **19/28**

The most common vulnerabilities in April:

Vulnerability	CWE number	Items
Out-of-bounds Read	CWE-125	4
Use After Free	CWE-416	4
OS Command Injection	CWE-78	3
Improper Input Validation	CWE-20	3
Out-of-bounds Write	CWE-787	3



ICSA-23-115-02: **Scada-LTS Third Party Component**

Medium level vulnerability: Cross-site Scripting.

[Scada-LTS Third Party Component | CISA]()

ICSA-23-115-01: **Keysight N8844A Data Analytics Web Service**

Critical level vulnerability: Deserialization of Untrusted Data.

[Keysight N8844A Data Analytics Web Service | CISA]()

ICSA-23-110-01: **INEA ME RTU**

Critical level vulnerability: OS Command Injection.

[INEA ME RTU | CISA]()

ICSA-23-108-02: **Schneider Electric Easy UPS Online Monitoring Software**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Handling of Case Sensitivity.

[Schneider Electric Easy UPS Online Monitoring Software | CISA]()

ICSA-23-108-01: **Omron CS/CJ Series**

High level vulnerability: Missing Authentication for Critical Function.

[Omron CS/CJ Series | CISA]()

ICSA-23-103-15: **Mitsubishi Electric India GC-ENET-COM**

High level vulnerability: Signal Handler Race Condition.

[Mitsubishi Electric India GC-ENET-COM | CISA]()

ICSA-23-103-14: **Datakit CrossCAD/Ware**

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

Datakit CrossCAD/Ware | CISA

ICSA-23-103-13: **Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families BadAlloc Vulnerabilities**

Critical level vulnerability: Integer Overflow or Wraparound.

Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families BadAlloc Vulnerabilities | CISA

ICSA-23-103-12: **Siemens Polarion ALM**

Medium level vulnerability: Improper Restriction of XML External Entity Reference.

Siemens Polarion ALM | CISA

ICSA-23-103-11: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerability: Stack-based Buffer Overflow.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-23-103-10: **Siemens Industrial Products**

High level vulnerabilities: Use After Free, Deadlock, Allocation of Resources Without Limits or Throttling.

Siemens Industrial Products | CISA

ICSA-23-103-09: **Siemens SCALANCE XCM332**

Critical level vulnerabilities: Allocation of Resources Without Limits or Throttling, Use After Free, Concurrent Execution Using Shared Resource with Improper Synchronization ('Race Condition'), Incorrect Default Permissions, Out-of-bounds Write, and Improper Validation of Syntactic Correctness of Input.

Siemens SCALANCE XCM332 | CISA

ICSA-23-103-08: **Siemens Mendix Forgot Password Module**

Medium level vulnerability: Observable Response Discrepancy.

Siemens Mendix Forgot Password Module | CISA

ICSA-23-103-07: **Siemens CPCI85 Firmware of SICAM A8000 Devices**

Critical level vulnerability: Improper Neutralization of Special Elements used in a Command ('Command Injection').

Siemens CPCI85 Firmware of SICAM A8000 Devices | CISA

ICSA-23-103-06: **Siemens SIPROTEC 5 Devices**

High level vulnerability: NULL Pointer Dereference.

Siemens SIPROTEC 5 Devices | CISA

ICSA-23-103-05: **Siemens SCALANCE X-200IRT Devices**

Medium level vulnerability: Inadequate Encryption Strength.

Siemens SCALANCE X-200IRT Devices | CISA

ICSA-23-103-04: **Siemens Path Traversal TIA Portal**

High level vulnerability: Improper Input Validation.

Siemens Path Traversal TIA Portal | CISA

ICSA-23-103-03: **Siemens in OPC Foundation Local Discovery Server**

High level vulnerability: Improper Input Validation.

Siemens in OPC Foundation Local Discovery Server | CISA

ICSA-23-103-02: **Siemens JT Open and JT Utilities**

High level vulnerability: Out-of-bounds Read.

Siemens JT Open and JT Utilities | CISA

ICSA-23-103-01: **Siemens Adaptec maxView Application**

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

Siemens Adaptec maxView Application | CISA

ICSA-23-101-01: **FANUC ROBOGUIDE-HandlingPRO**

Medium level vulnerability: Path Traversal.

FANUC ROBOGUIDE-HandlingPRO | CISA

ICSA-23-096-01: **Industrial Control Links ScadaFlex II SCADA Controllers**

Critical level vulnerability: External Control of File Name or Path.

Industrial Control Links ScadaFlex II SCADA Controllers | CISA

ICSA-23-096-02: **JTEKT ELECTRONICS Screen Creator Advance 2**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Use After Free.

JTEKT ELECTRONICS Screen Creator Advance 2 | CISA

ICSA-23-096-03: **JTEKT ELECTRONICS Kostac PLC Programming Software**

High level vulnerabilities: Out-of-bounds Read, Use After Free.

JTEKT ELECTRONICS Kostac PLC Programming Software | CISA

ICSA-23-096-04: **Korenix Jetwave**

High level vulnerabilities: Command Injection, Uncontrolled Resource Consumption.

Korenix Jetwave | CISA

ICSA-23-096-05: **Hitachi Energy MicroSCADA System Data Manager SDM600**

Critical level vulnerabilities: Unrestricted Upload of File with Dangerous Type, Improper Authorization, Improper Resource Shutdown or Release, Improper Privilege Management.

Hitachi Energy MicroSCADA System Data Manager SDM600 | CISA

ICSA-23-096-06: **mySCADA myPRO**

Critical level vulnerability: OS Command Injection.

mySCADA myPRO | CISA

ICSA-23-094-01: **Nexx Smart Home Device**

Critical level vulnerabilities: Use of Hard-coded Credentials, Authorization Bypass through User-controlled Key, Improper Input Validation, Improper Authentication.

Nexx Smart Home Device | CISA

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

Cybersecurity Alerts & Advisories | CISA

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

CISA has not published alerts in 2023 April.