2022 November, 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 2
ICS trainings, education 3
ICS conferences 9
ICS incidents 10
Book recommendation 11
ICS security news selection 12
ICS vulnerabilities 15
ICS alerts 22

ICS good practices, recommendations

ENISA Threat Landscape 2022

ENISA published a document, which contains the 2022 Global Threat Landscape. The overview details the following threats:

1. Ransomware
2. Malware
3. Social Engineering threats
4. Threats against data
5. Threats against availability: Denial of Service
6. Threats against availability: Internet threats
7. Disinformation – misinformation
8. Supply-chain attacks

The publication also has a critical infrastructure aspect. Heightened risk for Operational Technology networks. In ETL 2021, ENISA assessment was that the interest of state actors in targeting critical infrastructure and Operational Technology (OT) networks would certainly grow in the near future. Throughout the reporting period, ENISA assessment held valid as cyber operations targeting such infrastructure primarily for the collection of intelligence, deployment of newly observed ICS-targeting malware, and disruption were all observed.

Within Ukraine, the prime targets include the government and military networks and the energy and communications sectors from the perspective of critical infrastructure. Further disruptive operations could potentially spill-over to other countries.

Recommended to analyze the threats and react to the organizational aspects.

Source and more information available on the following link:

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

ICS trainings, education

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

Periodic online courses:

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

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

More details can be found on the following website:

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

ICS CERT offers the following courses:

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

More details can be found on the following website:

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

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours

- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

More details can be found on the following websites:

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

https://www.sans.org/cyber-security-courses/ics-visibility-detection-response/#training-and-pricing

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

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

More details can be found on the following website:

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

The **Department of Homeland Security's** two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

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

The **SCADAhacker.com** website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP or CEH, the course can help to add some ICS and SCADA specific knowledge.

Ethical Hacking for Industrial Control Systems

This exciting new and very advanced course supplies an environment to learn and apply offensive cyber operational (OCO) skills to a range of operational technology architectures. It introduces tactics, techniques, and procedures (TTP) to a range of real-world architectures, components, devices, and protocols that leverage both traditional software vulnerabilities and other more subtle, hard-to-find yet equally or more powerful human vulnerabilities that arise from typical system configuration and usage.

More details can be found on the following website:

https://scadahacker.com/training.html

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

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

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

More details can be found on the following website:

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

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three-day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel

- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

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

Bsigroup: Certified Lead SCADA Security Professional training course

This five-day training course will enable you to develop the expertise to plan, design and implement an effective programme to protect SCADA systems. You'll gain an understanding of common Industrial Control Systems (ICS) threats, vulnerabilities, and risks, and how they can be managed.

By attending this course you'll gain the knowledge and skills to advise on or manage risks related to SCADA environments and systems as a qualified professional. On successful completion of the PECB exam that takes place on the final day of this course, you'll gain Certified Lead SCADA Security Professional status.

Duration: 5 days, anytime at your office

More details can be found on the following website:

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

ICS/SCADA security training seminar

The courses are derived from 28 years of first-hand technology experience and industry best practices. The classes are customized to your team's requirements and taught at your offices, classrooms and online live by world-class instructors with publications, patents, awards/honours, and a passion to share knowledge.

More details can be found on the following website:

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

The Industrial Cyber Security Certification Course

This ICS Cybersecurity certification covers all aspects of Industrial Cyber security including a special advanced module on Understanding IEC 62443-2-4 that is very useful for not only automation system vendors and system integrators, but also to owners/operators to know what to expect from the vendor that supplies, installs, commissions and maintains the Industrial Control System.

When you complete the requirements of this course, you earn the title of CICP-Certified Industrial Cybersecurity Professional. (CICP)

More details can be found on the following website:

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

Secure IACS by ISA-IEC 62443 Standard

The subjects of this Udemy course: Security of Industrial Automation and Control Systems (IACS), IOT Security, OT Security, ISA-IEC 62443

Initially, the ISA99 committee considered IT standards and practices for use in the IACS. However, it was soon found that this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS.

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to address the need to improve the cybersecurity of IACS.

This course includes:

- 1.5 hours on-demand video
- 1 article
- 1 downloadable resource
- Full lifetime access
- Access on mobile and TV
- Certificate of completion

More details can be found on the following website:

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

NEW!

Dragos Academy ICS/OT Cybersecurity Training

Dragos Academy is a purpose-built training program, designed to teach the skills Dragos' own analysts, consultants, and practitioners use in the field to protect industrial and operational environments.

Strengthen your team's ICS cybersecurity skills with training from Dragos' world-class experts and improve their ability to prevent, detect, and respond to cyber attacks in your OT environment. Hands-on training is instructor-led and in a classroom or virtual setting. On-demand training is available to Dragos customers anytime, anywhere.

This two-day course is designed for IT professionals tasked with learning ICS/OT cybersecurity, or for ICS/OT professionals who want to learn more about how IT

concepts apply in industrial networks. This course will provide you with the ICS/OT subject-matter foundation necessary to advance into the Dragos Certified User training.

More details can be found on the following website:

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

ICS conferences

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

Healthcare Cybersecurity Forum

The HIMSS 2022 Healthcare Cybersecurity Forum will explore how the industry is protecting itself today and how it must evolve for the future.

The agenda will include a mix of business and technology focused sessions highlighting topics such as:

- Workforce and organizational culture challenges
- Balancing security and risk decisions
- Communications and preparedness
- Keeping up with technology, public policy and threat landscapes.

You'll be immersed in interactive workshops—like "Healthcare Technology Crisis Simulation" and "Medical Device Cybersecurity Threat Modeling", sessions with practical applications and best practices, plus unparalleled, quality networking time with fellow cybersecurity professionals.

Boston MA, USA; 5th – 6th December 2022

More details can be found on the following website:

https://www.himss.org/event-healthcare-cybersecurity-forum

World Congress on Industrial Control Systems Security

The 8th World Congress on Industrial Control Systems Security (WCICSS-2022) is a meeting point for professionals and researchers, IT security professionals, managers, developers, educators, vendors and service providers who are involved in development, integration, assessment, implementation, and operation of industrial cybersecurity technologies. The WCICSS is an international refereed conference dedicated to the advancement of the theory and practices of Industrial Controls Security and SCADA. Therefore, the conference will provide opportunities to discuss both the current status and emerging trends in protection of industrial control systems.

London, UK (Virtual Conference), 6th – 8th December 2022

More details can be found on the following website:

https://wcicss.org/

ICS incidents

Indian Energy Company hit by cyberattack

India's largest integrated power company suffered a cyberattack in October. The company informed the media that some of the IT systems affected in the cyberattack. The Mumbai-based electric utility company, part of the Tata Group conglomerate didn't share any other details.

Tata Power serves more than 12 million customers through its distributors. The attacks were attributed to an emerging threat cluster Recorded Future is tracking under the name Threat Activity Group 38 (TAG-38).

The aim of the attack is gathering more information from the critical infrastructure according to the Company.

The Hive ransomware group a few days later has claimed responsibility for the recent cyberattack on Tata Power, a leading Indian energy company, and has started leaking stolen employee data.

The Hive ransomware group started leaking data probably the reason that the Company didn't pay.

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

https://thehackernews.com/2022/10/indian-energy-company-tata-powers-it.html

https://techcrunch.com/2022/10/25/tata-power-hive-ransomware/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYmluZy5jb20v&guce_referrer_sig=AQAAAKNpTDN6TX-Xg2oo1RInAZFzYPuceZbcuscgdnYDt4rykPNXnf1wAzWFQF_86AIh3jSC9nuaSe3J9s8DJ7sqk2E5GngMqfmeiFKY5DMW-EJoBCge04DekHCM2Ggjjba-7iqZKDOoMD1zEBPf8pmKMiNHQq1I1tTlKZWIYfu1xLGc

Book recommendation

Critical Infrastructure Security and Resilience

This book presents the latest trends in attacks and protection methods of Critical Infrastructure. It describes original research models and applied solutions for protecting against major emerging threats in Critical Infrastructure and their underlying networks. It presents a number of emerging endeavors, from newly adopted technical expertise in industrial security to efficient modeling and implementation of attacks and relevant security measures in industrial control systems; including advancements in hardware and services security, interdependency networks, risk analysis, and control systems security along with their underlying protocols.

Novel attacks against Critical Infrastructure (CI) demand novel security solutions. Simply adding more of what is done already (e.g., more thorough risk assessments, more expensive Intrusion Prevention/Detection Systems, more efficient firewalls, etc.) is simply not enough against threats and attacks that seem to have evolved beyond modern analyses and protection methods.

The knowledge presented here will help Critical Infrastructure authorities, security officers, Industrial Control Systems (ICS) personnel and relevant researchers to

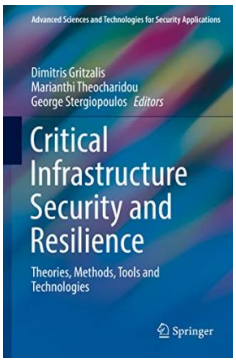
- get acquainted with advancements in the field,
- integrate security research into their industrial or research work,
- evolve current practices in modeling and analyzing Critical Infrastructures, and
- moderate potential crises and emergencies influencing or emerging from Critical Infrastructure.

Authors/Editors: Dimitris Gritzalis, Marianthi Theocharidou, George Stergiopoulos

Year of issue: 2019

The book is available at the following link:

https://www.amazon.de/-/en/Dimitris-Gritzalis-ebook/dp/B07FVN6PCF



ICS security news selection

White House Adds Chemical Sector to ICS Cybersecurity Initiative

The White House announced on Wednesday that the Industrial Control Systems (ICS) Cybersecurity Initiative has been expanded to include the chemical sector.

The ICS Cybersecurity Initiative was first announced in July 2021 — after the disruptive attack on Colonial Pipeline — and its goal is to improve critical infrastructure security by encouraging and facilitating the deployment of threat detection technologies and systems.

Chemical is the fourth sector added to the initiative, after electric, pipeline and water. Chemical organizations can analyze the best practices and lessons learned from these other sectors and create a cybersecurity action plan for the next 100 days. …

Source and more information:

https://www.securityweek.com/white-house-adds-chemical-sector-ics-cybersecurity-initiative

Maple Leaf Foods suffers outage following weekend cyberattack

Maple Leaf Foods confirmed on Sunday that it experienced a cybersecurity incident causing a system outage and disruption of operations.

Maple Leaf Foods is Canada's largest prepared meats and poultry food producer, operating 21 manufacturing facilities, employing 14,000 people, and contracting over 700 barns. In 2021, the firm generated $3.3 billion in sales.

Hackers often launch cyberattacks during weekends, hoping to find incident responders understaffed, and maximize their chances for success. …

Source and more information:

https://www.bleepingcomputer.com/news/security/maple-leaf-foods-suffers-outage-following-weekend-cyberattack/

IoT devices can undermine your security. Here are four ways to boost your defences

Connected Internet of Things (IoT) devices such as printers, cameras and routers are leaving networks vulnerable to cyberattacks because they're not being properly secured.

And it isn't just home and office networks that are being left open to exploitation by malicious hackers targeting the Internet of Things – critical infrastructure is also vulnerable too because IoT security isn't being managed correctly, potentially leaving industrial control systems exposed, Microsoft has warned. …

Source and more information:

https://www.zdnet.com/article/iot-devices-can-undermine-your-security-here-are-four-ways-to-boost-your-defences/

Key cybersecurity trends in the energy sector

The key trends for the energy industry are about how we manage the future supply and demand challenges at a much more granular level than we are currently able to do. If we're ever to balance the supply and demand equation against the backdrop of increased consumer demands (electric vehicles, mass transport systems, electrification of home heating systems, etc.), and the increased complexity in the generation, distribution and storage systems, this supply and demand will have to base its existence on an increase in interconnectivity and information sharing between all these elements to make them work. …

Source and more information:

https://www.helpnetsecurity.com/2022/11/14/energy-sector-cybersecurity-trends-video/

Risk Mitigation Strategies to Close the XIoT Security Gap

After more than 20 years of connecting devices to the Internet, we've reached the point where our physical world is very dependent on its digital components. We now have direct connections to process control systems and smart sensors in industrial environments, medical imaging equipment and patient monitoring systems in healthcare organizations, and other devices used in smart grids and building management systems. Even our most basic needs like food and water depend on

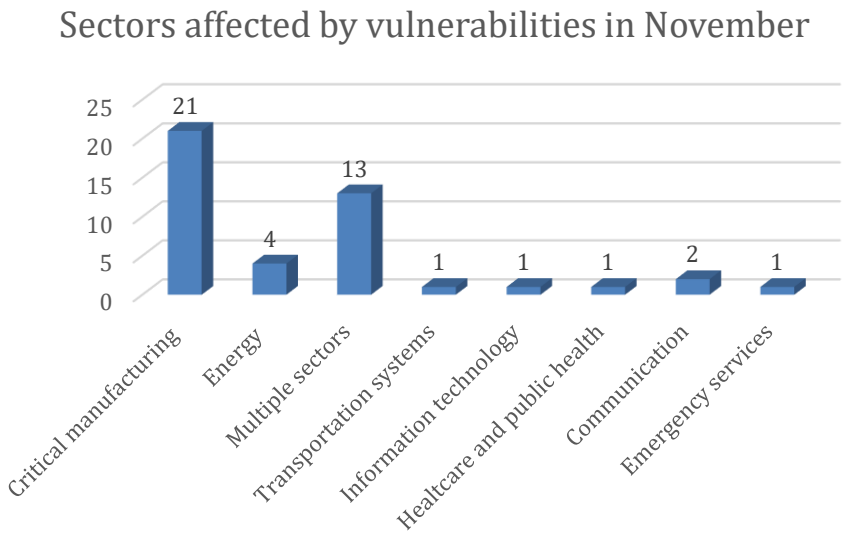
cyber-physical systems (CPS) and the connected devices that underpin them, referred to holistically as the Extended Internet of Things (XIoT). But many of these connected devices were not necessarily designed with security in mind. This is par for the course with technology innovation and will take years, if not decades, before a new generation of connected assets emerges with more natively integrated security processes and pathways. …

Source and more information:

https://www.securityweek.com/risk-mitigation-strategies-close-xiot-security-gap

ICS vulnerabilities

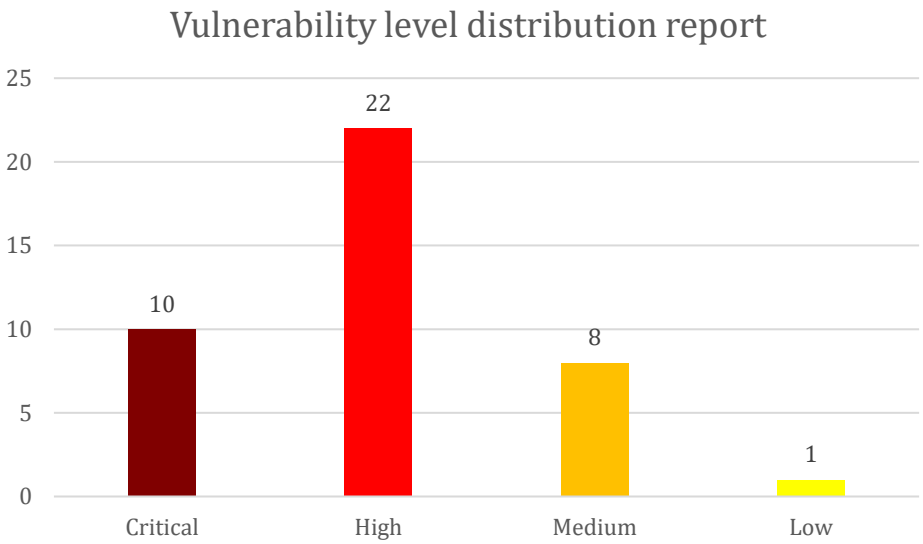
In November 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:



Average number of vulnerabilities per vulnerability report in November: **1,92**

The most common vulnerabilities in November:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	5
Out-of-bounds Read	CWE-125	5
Cross-site Scripting	CWE-79	4
Uncontrolled Resource Consumption	CWE-400	4
Out-of-bounds Write	CWE-787	4



ICSA-22-333-01: **Mitsubishi Electric GOT2000**

Medium level vulnerability: Improper Input Validation.

Mitsubishi Electric GOT2000 | CISA

ICSA-22-333-02: **Hitachi Energy IED Connectivity Packages and PCM600 Products**

High level vulnerability: Cleartext Storage of Sensitive Information.

Hitachi Energy IED Connectivity Packages and PCM600 Products | CISA

ICSA-22-333-03: **Hitachi Energy MicroSCADA Pro/X SYS600 Products**

High level vulnerability: Improper Input Validation.

Hitachi Energy MicroSCADA Pro/X SYS600 Products | CISA

ICSA-22-333-04: **Moxa UC Series**

High level vulnerability: Improper Physical Access Control.

Moxa UC Series | CISA

ICSA-22-333-05: **Mitsubishi Electric FA Engineering Software**

Critical level vulnerabilities: Cleartext Storage of Sensitive Information, Use of Hard-coded Password, Insufficiently Protected Credentials, Use of Hard-coded Cryptographic Key, Cleartext Storage of Sensitive Information in Memory.

Mitsubishi Electric FA Engineering Software | CISA

ICSA-21-334-02: **Mitsubishi Electric MELSEC and MELIPC Series (Update E)**

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.

Mitsubishi Electric MELSEC and MELIPC Series (Update E) | CISA

ICSA-19-346-02: **Omron PLC CJ and CS Series (Update A)**

High level vulnerabilities: Authentication Bypass by Spoofing, Authentication Bypass by Capture-replay, Unrestricted Externally Accessible Lock.

Omron PLC CJ and CS Series (Update A) | CISA

ICSA-22-326-01: **AVEVA Edge**

Critical level vulnerabilities: Uncontrolled Search Path Element, Exposure of Sensitive Information to an Unauthorized Actor, Uncontrolled Resource Consumption, Improper Access Control, Windows UNC Share.

AVEVA Edge | CISA

ICSA-22-326-02: **Digital Alert Systems DASDEC**

Low level vulnerability: Cross-site Scripting.

Digital Alert Systems DASDEC | CISA

ICSA-22-326-03: **Phoenix Contact Automation Worx**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Read.

Phoenix Contact Automation Worx | CISA

ICSA-22-326-04: **GE CIMPLICITY**

High level vulnerabilities: Access of Uninitialized Pointer, Heap-based Buffer Overflow, Untrusted Pointer Dereference, Out-of-bounds Write.

GE CIMPLICITY | CISA

ICSA-22-326-05: **Moxa Multiple ARM-Based Computers**

High level vulnerability: Privilege Escalation.

Moxa Multiple ARM-Based Computers | CISA

ICSA-21-049-02: **Mitsubishi Electric FA Engineering Software Products (Update G)**

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

Mitsubishi Electric FA Engineering Software Products (Update G) | CISA

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

High level vulnerability: Unquoted Search Path or Element.

Mitsubishi Electric Factory Automation Engineering Products (Update I) | CISA

ICSMA-21-152-01: **Hillrom Medical Device Management (Update C)**

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

Hillrom Medical Device Management (Update C) | CISA

ICSA-22-321-01: **Red Lion Crimson**

High level vulnerability: Path Traversal.

Red Lion Crimson | CISA

ICSA-22-321-02: **Cradlepoint IBR600**

High level vulnerability: Command Injection.

Cradlepoint IBR600 | CISA

ICSA-22-319-01: **Mitsubishi Electric GT SoftGOT2000**

Critical level vulnerability: Operating System (OS) Command Injection.

Mitsubishi Electric GT SoftGOT2000 | CISA

ICSA-22-314-03: **Siemens SINEC Network Management System Logback Component**

Medium level vulnerability: Deserialization of Untrusted Data.

Siemens SINEC Network Management System Logback Component | CISA

ICSA-22-314-01: **Siemens Parasolid**

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

Siemens Parasolid | CISA

ICSA-22-314-02: **Siemens Web Server Login Page of Industrial Controllers**

Medium level vulnerability: Cross-Site Request Forgery (CSRF).

Siemens Web Server Login Page of Industrial Controllers | CISA

ICSA-22-314-04: **Siemens SINUMERIK ONE and SINUMERIK MC**

Critical level vulnerability: Insufficiently Protected Credentials.

Siemens SINUMERIK ONE and SINUMERIK MC | CISA

ICSA-22-314-05: **Siemens RUGGEDCOM ROS**

Medium level vulnerability: Uncontrolled Resource Consumption.

Siemens RUGGEDCOM ROS | CISA

ICSA-22-314-06: **Siemens QMS Automotive**

High level vulnerability: Cleartext Storage of Sensitive Information in Memory.

Siemens QMS Automotive | CISA

ICSA-22-314-07: **Omron NJ/NX-series Machine Automation Controllers**

High level vulnerability: Active Debug Code.

Omron NJ/NX-series Machine Automation Controllers | CISA

ICSA-22-314-08: **Omron NJ/NX-series Machine Automation Controllers**

Critical level vulnerabilities: Hard-coded Credentials, Authentication Bypass by Capture-replay.

Omron NJ/NX-series Machine Automation Controllers | CISA

ICSA-22-314-09: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: Heap-based Buffer Overflow, Out-of-bounds Write, Out-of-bounds Read, Use After Free, Stack-based Buffer Overflow.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-22-314-10: **Siemens SCALANCE W1750D**

Critical level vulnerabilities: Uncontrolled Resource Consumption, Buffer Copy without Checking Size of Input, Improper Neutralization of Input During Web Page Generation, Improper Neutralization of Special Elements used in a Command, Improper Input Validation.

Siemens SCALANCE W1750D | CISA

ICSA-22-314-11: **Siemens SICAM Q100**

Critical level vulnerabilities: Session Fixation, Improper Input Validation.

Siemens SICAM Q100 | CISA

ICSA-21-350-06: **Siemens Capital VSTAR (Update A)**

High level vulnerabilities: Access of Resource Using Incompatible Type, Improper Validation of Specified Quantity in Input, Out-of-Bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Null Termination, Integer Underflow, Improper Handling of Inconsistent Structural Elements.

Siemens Capital VSTAR (Update A) | CISA

ICSA-22-286-15: **Siemens SCALANCE X-200 and X-200IRT Families (Update A)**

Critical level vulnerability: Cross-site Scripting.

Siemens SCALANCE X-200 and X-200IRT Families (Update A) | CISA

ICSA-22-258-03: **Siemens RUGGEDCOM ROS (Update A)**

Medium level vulnerability: Uncontrolled Resource Consumption.

Siemens RUGGEDCOM ROS (Update A) | CISA

ICSA-22-228-02: **LS ELECTRIC PLC and XG5000 (Update A)**

Medium level vulnerability: Inadequate Encryption Strength.

LS ELECTRIC PLC and XG5000 (Update A) | CISA

ICSA-22-298-06: **Delta Electronics DIAEnergie (Update A)**

High level vulnerabilities: Cross-site Scripting, SQL Injection.

Delta Electronics DIAEnergie (Update A) | CISA

ICSA-22-258-04: **Siemens Mendix SAML Module (Update A)**

High level vulnerability: Authentication Bypass by Capture-replay.

Siemens Mendix SAML Module (Update A) | CISA

ICSA-22-286-11: **Siemens SCALANCE and RUGGEDCOM Products (Update A)**

High level vulnerability: Missing Authorization.

Siemens SCALANCE and RUGGEDCOM Products (Update A) | CISA

ICSA-21-350-13: **Siemens Questa and ModelSim (Update A)**

Critical level vulnerability: Insufficiently Protected Credentials.

Siemens Questa and ModelSim (Update A) | CISA

ICSA-22-069-01: **Siemens RUGGEDCOM Devices (Update C)**

Medium level vulnerability: Inadequate Encryption Strength.

Siemens RUGGEDCOM Devices (Update C) | CISA

ICSA-22-307-01: **ETIC Telecom Remote Access Server (RAS)**

Critical level vulnerabilities: Insufficient Verification of Data Authenticity, Path Traversal, Unrestricted Upload of File with Dangerous Type.

ETIC Telecom Remote Access Server (RAS) | CISA

ICSA-22-307-02: **Nokia ASIK AirScale System Module**

High level vulnerabilities: Improper Access Control for Volatile Memory Containing Boot Code, Assumed-Immutable Data is Stored in Writable Memory.

Nokia ASIK AirScale System Module | CISA

ICSA-22-307-03: **Delta Industrial Automation DIALink**

High level vulnerability: Path traversal.

Delta Industrial Automation DIALink | CISA

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 November 2022, ICS-CERT has published an alert:

Hive Ransomware

This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) are releasing this joint CSA to disseminate known Hive IOCs and TTPs identified through FBI investigations as recently as November 2022.

FBI, CISA, and HHS encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents. Victims of ransomware operations should report the incident to their local FBI field office or CISA.

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

https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

The full report is available here:

https://www.cisa.gov/uscert/sites/default/files/publications/aa22-321a_joint_csa_stopransomware_hive.pdf