2023 March, Industrial Control Systems security feed

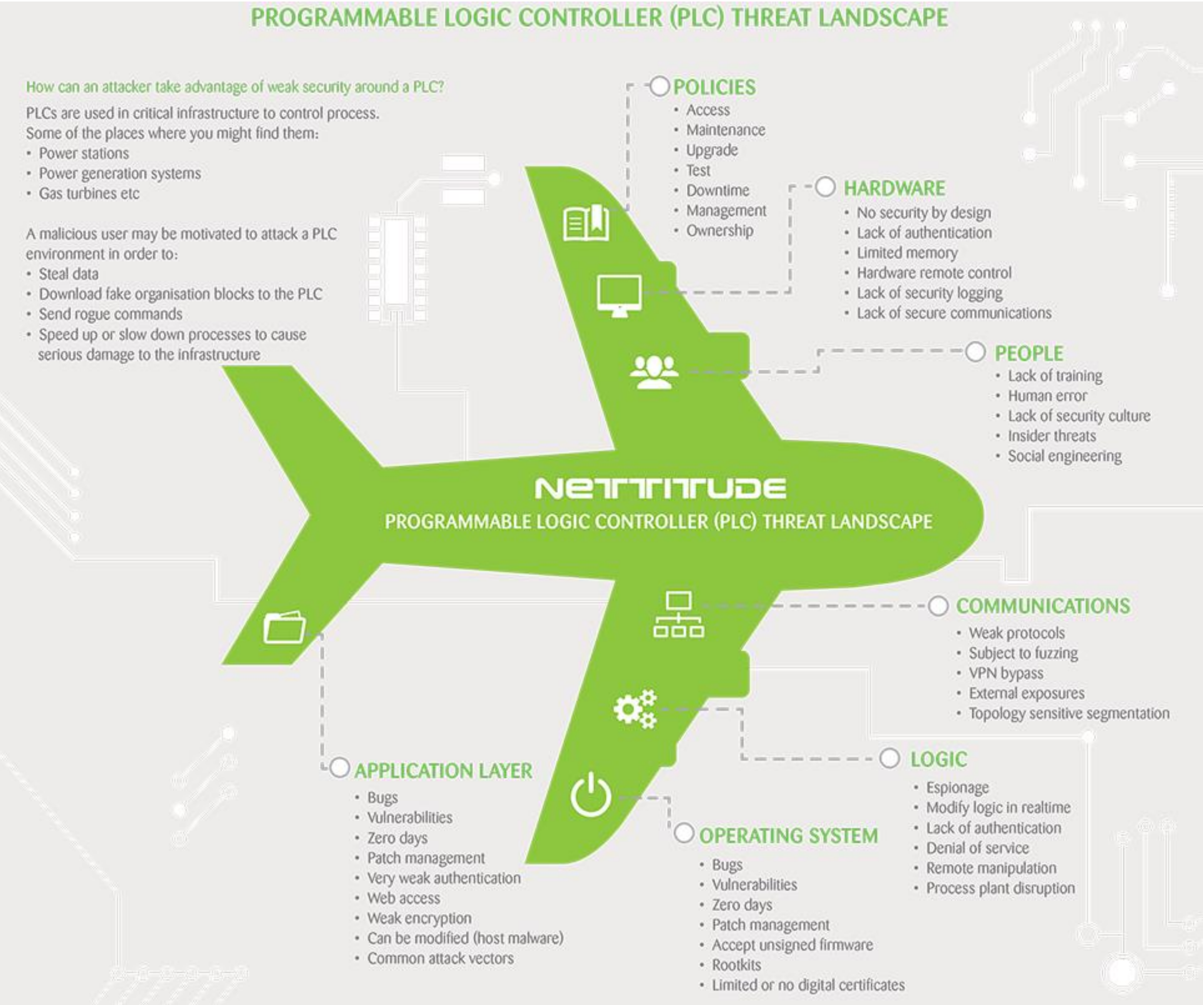
Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, 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

PLC Threat Landscape

Nettitude published in 2015 a PLC (Programmable Logic Controller Threat Landscape picture, which is nowadays also useful and good to identify the potential threats and analyse the risks.



PROGRAMMABLE LOGIC CONTROLLER (PLC) THREAT LANDSCAPE

How can an attacker take advantage of weak security around a PLC?

PLCs are used in critical infrastructure to control process. Some of the places where you might find them:

- Power stations
- Power generation systems
- Gas turbines etc

A malicious user may be motivated to attack a PLC environment in order to:

- Steal data
- Download fake organisation blocks to the PLC
- Send rogue commands
- Speed up or slow down processes to cause serious damage to the infrastructure

NETTITUDE
PROGRAMMABLE LOGIC CONTROLLER (PLC) THREAT LANDSCAPE

POLICIES

- Access
- Maintenance
- Upgrade
- Test
- Downtime
- Management
- Ownership

HARDWARE

- No security by design
- Lack of authentication
- Limited memory
- Hardware remote control
- Lack of security logging
- Lack of secure communications

PEOPLE

- Lack of training
- Human error
- Lack of security culture
- Insider threats
- Social engineering

COMMUNICATIONS

- Weak protocols
- Subject to fuzzing
- VPN bypass
- External exposures
- Topology sensitive segmentation

LOGIC

- Espionage
- Modify logic in realtime
- Lack of authentication
- Denial of service
- Remote manipulation
- Process plant disruption

OPERATING SYSTEM

- Bugs
- Vulnerabilities
- Zero days
- Patch management
- Accept unsigned firmware
- Rootkits
- Limited or no digital certificates

APPLICATION LAYER

- Bugs
- Vulnerabilities
- Zero days
- Patch management
- Very weak authentication
- Web access
- Weak encryption
- Can be modified (host malware)
- Common attack vectors

Source and more information available on the following link:

https://blog.nettitude.com/uk/programmable-logic-controller-security

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in April 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 April 2023, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

#CS4CA Cyber Security for Critical Assets

The critical infrastructure that provides our energy, utilities, healthcare and other basic foundations of our societies is fundamentally changing. As we continue to move our traditional technologies online, our IT and OT systems face increasingly significant risks. Meanwhile, challenges emerging from an increasing cybersecurity skills gap, new regulations and today’s geopolitical issues emphasise the need to place cyber security at the forefront of our businesses’ concerns. Providing the collaboration platform and expertise needed to address these ever-increasing challenges, the globally acclaimed Cyber Security for Critical Assets summit returns to Singapore for its 4th Asian Pacific edition in 2023.

Singapore, Singapore; 18th – 19th April 2023

More details can be found on the following website:

https://apac.cs4ca.com/

ICS Security Summit & Training 2023

The annual ICS Security Summit brings together the industry's top practitioners and leading experts from around the globe to share actionable ideas, methods, and techniques for safeguarding critical infrastructure. In-depth talks and interactive sessions will deliver proven advances and approaches that make a real difference for the individuals engaged in this fight every day.

Two days of highly technical talks and panel discussions, ICS Solutions Track and Expo Hall, GRID NetWars and other exciting programs.

Orlando, FL, US and Virtual – ET; 30th April – 8th May 2023

More details can be found on the following website:

https://www.sans.org/cyber-security-training-events/ics-security-summit-2023/

ICS incidents

Hacker attack on Enercity

The Hanover-based energy company Enercity was the target of a hacker attack in October of 2022. Enercity announced on its homepage the following: "Our security systems reacted immediately so that greater damage to the company could be averted," it stated. The most important message was that the critical infrastructure had not been affected: "Our grids and power plants are running stably and security of supply is guaranteed, we keep supplying all our customers." There are reportedly restrictions on customer service.

The attack comes days after Germany's federal cybersecurity office warned that the threat situation facing the country was "higher than ever."

The energy sector in Germany has been repeatedly targeted by criminals in recent months.

Several cyber incidents preceding the Russian invasion of Ukraine in February affected the oil and chemical sector in the country — as well as in Germany's neighbours — provoking concerns that they were part of a criminal campaign coordinated by Russian intelligence.

The sources are available on the following links:

https://www.energate-messenger.com/news/227628/hacker-attack-on-enercity

https://therecord.media/major-german-energy-supplier-hit-by-cyberattack

Book recommendation

OT operational technology Third Edition

This OT operational technology Guide is unlike the books you're used to. If you're looking for a textbook, this might not be for you. This book and its included digital components are for you, who understands the importance of asking great questions. This gives you the questions to uncover the OT operational technology challenges you're facing and generate better solutions to solve those problems.

Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department.

Unless you're talking a one-time, single-use project, there should be a process. That process needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?'

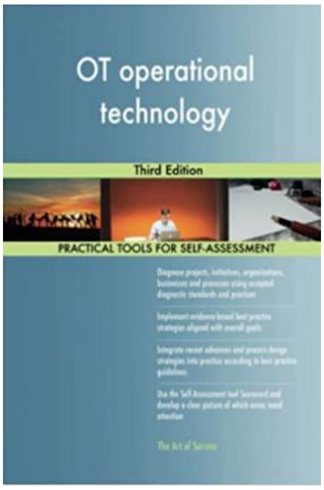
This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make OT operational technology investments work better.

Authors/Editors: Gerardus Blokdyk (Author)

Year of issue: 2022

The book is available at the following link:

https://www.amazon.com/Operational-Technology-Third-Gerardus-Blokdyk/dp/0655436030


OT operational technology
Third Edition
PRACTICAL TOOLS FOR SELF-ASSESSMENT

ICS security news selection

EPA Mandates States Report on Cyber Threats to Water Systems

The Biden administration on Friday said it would require states to report on cybersecurity threats in their audits of public water systems, a day after it released a broader plan to protect critical infrastructure against cyberattacks.

The Environmental Protection Agency said public water systems are increasingly at risk from cyberattacks that amount to a threat to public health.

"Cyberattacks against critical infrastructure facilities, including drinking water systems, are increasing, and public water systems are vulnerable," said EPA Assistant Administrator Radhika Fox. "Cyberattacks have the potential to contaminate drinking water.". ...

Source, and more information:

https://www.securityweek.com/epa-mandates-states-report-on-cyber-threats-to-water-systems/

UK won the Military Cyberwarfare exercise Defence Cyber Marvel 2 (DCM2)

The Defence Cyber Marvel 2 (DCM2) is the largest training exercise organised by the Army Cyber Association to allow personnel from across the Armed Forces to build their skills within the cyber and electromagnetic domain.

This year, 750 cyber specialists have participated in the military cyberwarfare exercise. 34 teams from 11 countries, including India, Italy, Ghana, Japan, US, Ukraine, Kenya, and Oman, have taken part in a live-fire cyber battle that lasted seven days.

"Organised by a team of cyber specialists from the British Army, Defence Cyber Marvel 2 (DCM2) was the culmination of more than 12 months of training for more than 750 cyber specialists, including Defence personnel, government agencies, industry partners, and other nations." reads the press release published by the UK Ministry of Defence.

The exercise was hosted in Tallinn, Estonia, participant teams were involved in common and complex simulations of attacks against IT and OT networks, and unmanned robotic systems. The exercise also simulated some of the tactics Russia used to disrupt Ukrainian cyberspace amid the beginning of the invasion one year ago. ...

Source, and more information:

https://securityaffairs.com/142669/cyber-warfare-2/uk-won-defence-cyber-marvel-2-dcm2.html

ChatGPT Integrated Into Cybersecurity Products as Industry Tests Its Capabilities

While there has been a lot of talk about how OpenAI's ChatGPT could be abused for malicious purposes and how it can pose a threat, the artificial intelligence chatbot can also be very useful to the cybersecurity industry.

Launched in November 2022, ChatGPT has been described by many as revolutionary. It is built on top of OpenAI's GPT-3 family of large language models and users interact with it through prompts.

There have been numerous articles describing how ChatGPT's capabilities can be used for malicious purposes, including to write credible phishing emails and create malware.

However, ChatGPT can bring many benefits to defenders as well, and the cybersecurity industry has been increasingly integrating it into products and services. In addition, some members of the industry have been testing its capabilities and limitations. …

Source, and more information:

https://www.securityweek.com/chatgpt-integrated-into-cybersecurity-products-as-industry-tests-its-capabilities/

US Electric Cooperative Association Launches Commercial OT Security Solution

The National Rural Electric Cooperative Association (NRECA) this week announced the commercial launch of its operational technology (OT) cybersecurity solution.

NRECA is a national trade association that represents roughly 900 local electric cooperatives in the United States. Its cybersecurity solution, named Essence, has been in development since 2014 with funding from the US Department of Energy.

NRECA announced in 2020 that it had received $6 million from the Energy Department to develop Essence 2.0. In January 2023, it unveiled Essence 3.0 and announced that Essence would be going from an R&D project funded by the Energy Department to a commercial solution.

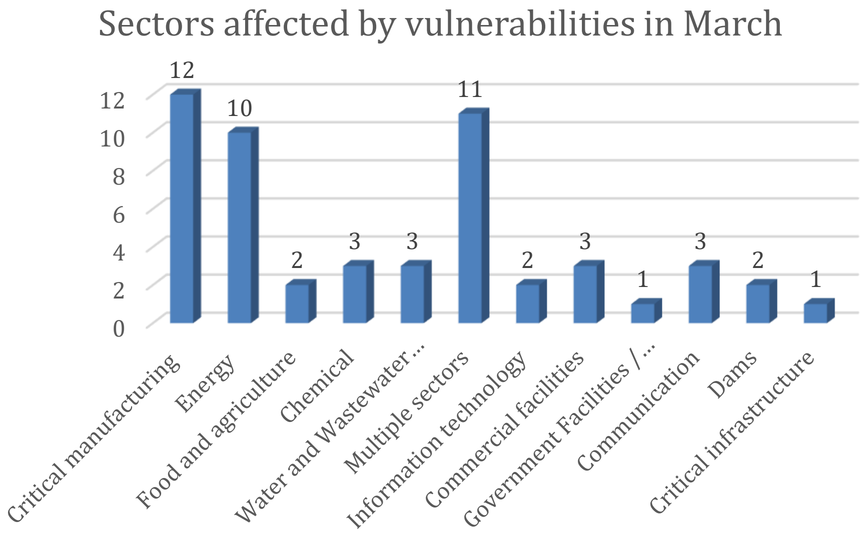
The organization officially announced the commercial launch of Essence on the 27th of February, 2023. The solution has already been used by dozens of electric cooperatives, but it can be deployed at other types of utilities as well, including gas and water providers.

Source, and more information:

https://www.securityweek.com/us-electric-cooperative-association-launches-commercial-ot-security-solution/

ICS vulnerabilities

In March 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:

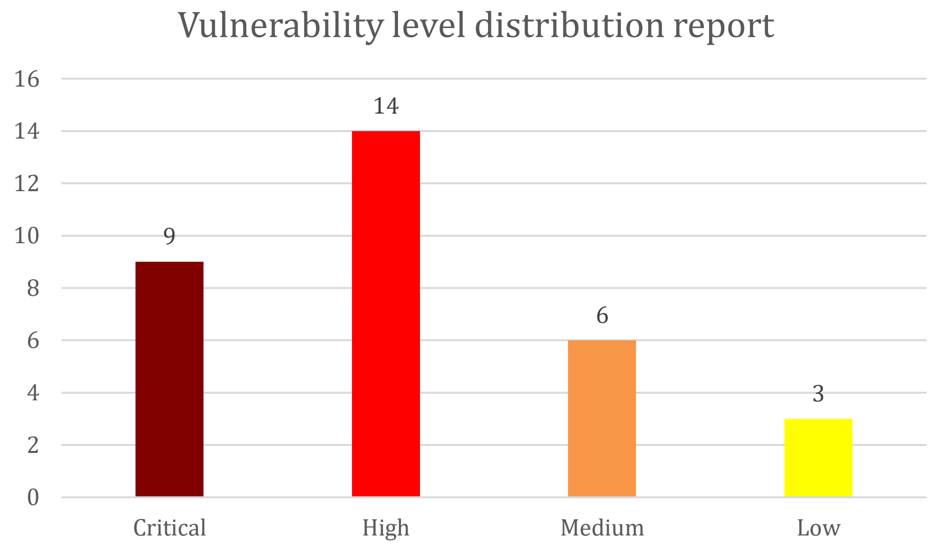


Average number of vulnerabilities per vulnerability report in March: **3,18**

Vulnerabilities/Exploitable remotely: **32/23**

The most common vulnerabilities in March:

Vulnerability	CWE number	Items
Improper Authentication	CWE-287	4
Improper Input Validation	CWE-20	4
Missing Authentication for Critical Function	CWE-306	4
Use After Free	CWE-416	4
Improper Access Control	CWE-284	4
Command injection	CWE-77	4
Improper Authentication	CWE-287	4



ICSA-23-089-01: **Hitachi Energy IEC 61850 MMS-Server**

Medium level vulnerability: Improper Resource Shutdown or Release.

Hitachi Energy IEC 61850 MMS-Server | CISA

ICSA-23-082-06: **ProPump and Controls Osprey Pump Controller**

Critical level vulnerabilities: Insufficient Entropy, Use of GET Request Method with Sensitive Query Strings, Use of Hard-coded Password, OS Command Injection, Cross-site Scripting, Authentication Bypass using an Alternate Path or Channel, Cross-Site Request Forgery, Command Injection.

ProPump and Controls Osprey Pump Controller | CISA

ICSA-23-082-05: **ABB Pulsar Plus Controller**

Medium level vulnerabilities: Use of Insufficiently Random Values, Cross-Site Request Forgery (CSRF).

ABB Pulsar Plus Controller | CISA

ICSA-23-082-04: **Schneider Electric IGSS**

High level vulnerabilities: Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity, Deserialization of Untrusted Data, Improper Limitation of a Pathname to a Restricted Directory, and Improper Input Validation.

Schneider Electric IGSS | CISA

ICSA-23-082-03: **SAUTER EY-modulo 5 Building Automation Stations**

High level vulnerabilities: Cross-site Scripting, Cleartext Transmission of Sensitive Information, and Unrestricted Upload of File with Dangerous Type.

SAUTER EY-modulo 5 Building Automation Stations | CISA

ICSA-23-082-02: **CP Plus KVMS Pro**

High level vulnerability: Insufficiently Protected Credentials.

CP Plus KVMS Pro | CISA

ICSA-23-082-01: **RoboDK**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

RoboDK | CISA

ICSA-23-080-07: **Siemens SCALANCE Third-Party**

High level vulnerabilities: Generation of Error Message Containing Sensitive Information, Out-of-bounds Write, NULL Pointer Dereference, Out-of-bounds Read, Improper Input Validation, Release of Invalid Pointer or Reference, Use After Free, Prototype Pollution.

Siemens SCALANCE Third-Party | CISA

ICSA-23-080-06: **Rockwell Automation ThinManager**

Critical level vulnerabilities: Path Traversal, Heap-Based Buffer Overflow.

Rockwell Automation ThinManager | CISA

ICSA-23-080-05: **VISAM VBASE Automation Base**

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

VISAM VBASE Automation Base | CISA

ICSA-23-080-04: **Siemens RADIUS Client of SIPROTEC 5 Devices**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

Siemens RADIUS Client of SIPROTEC 5 Devices | CISA

ICSA-23-080-03: **Siemens RUGGEDCOM APE1808 Product Family**

High level vulnerability: Time-of-check Time-of-use (TOCTOU) Race Condition.

Siemens RUGGEDCOM APE1808 Product Family | CISA

ICSA-23-080-02: **Delta Electronics InfraSuite Device Master**

Critical level vulnerabilities: Deserialization of Untrusted Data, Improper Access Control, Exposed Dangerous Method or Function, Path Traversal, Improper Authentication, Command Injection, Incorrect Permission Assignment for Critical Resource, Missing Authentication for Critical Function.

Delta Electronics InfraSuite Device Master | CISA

ICSA-23-080-01: **Keysight N6845A Geolocation Server**

High level vulnerability: Deserialization of Untrusted Data.

Keysight N6845A Geolocation Server | CISA

ICSA-23-075-07: **Rockwell Automation Modbus TCP AOI Server**

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

Rockwell Automation Modbus TCP AOI Server | CISA

ICSA-23-075-06: **Honeywell OneWireless Wireless Device Manager**

Critical level vulnerabilities: Command Injection, Use of Insufficiently Random Values, Missing Authentication for Critical Function.

Honeywell OneWireless Wireless Device Manager | CISA

ICSA-23-075-05: **Siemens Mendix SAML Module**

Critical level vulnerability: Incorrect Implementation of Authentication Algorithm.

Siemens Mendix SAML Module | CISA

ICSA-23-075-04: **Siemens SCALANCE W1750D Devices**

High level vulnerabilities: Inadequate Encryption Strength, Double Free, Use After Free, Improper Input Validation.

Siemens SCALANCE W1750D Devices | CISA

ICSA-23-075-03: **Siemens RUGGEDCOM CROSSBOW V5.2**

Medium level vulnerability: Missing Authorization.

Siemens RUGGEDCOM CROSSBOW V5.2 | CISA

ICSA-23-075-02: **Siemens RUGGEDCOM CROSSBOW V5.3**

High level vulnerabilities: Missing Authorization, SQL Injection.

Siemens RUGGEDCOM CROSSBOW V5.3 | CISA

ICSA-23-075-01: **Siemens SCALANCE, RUGGEDCOM Third-Party**

Critical level vulnerabilities: Out-of-bounds Write, Exposure of Sensitive Information to an Unauthorized Actor, Improper Locking, Improper Input Validation, NULL Pointer Dereference, Out-of-bounds Read, Release of Invalid Pointer or Reference, Use After Free, Improper Authentication, OS Command Injection, Improper Certificate Validation, Improper Resource Shutdown or Release, Race Condition, Uncaught Exception, Integer Underflow (Wrap or Wraparound), Classic Buffer Overflow, Double Free, Incorrect Authorization, Allocation of Resources Without Limits or Throttling, Improper Validation of Syntactic Correctness of Input.

Siemens SCALANCE, RUGGEDCOM Third-Party | CISA

ICSA-23-073-04: **AVEVA Plant SCADA and AVEVA Telemetry Server**

Critical level vulnerability: Improper Authorization.

AVEVA Plant SCADA and AVEVA Telemetry Server | CISA

ICSA-23-073-03: **GE iFIX**

High level vulnerability: Code Injection.

GE iFIX | CISA

ICSA-23-073-02: **Autodesk FBX SDK**

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

Autodesk FBX SDK | CISA

ICSA-23-073-01: **Omron CJ1M PLC**

Critical level vulnerability: Improper Access Control.

Omron CJ1M PLC | CISA

ICSA-23-068-05: **Hitachi Energy Relion 670, 650 and SAM600-IO Series**

Low level vulnerability: Insufficient Verification of Data Authenticity.

Hitachi Energy Relion 670, 650 and SAM600-IO Series | CISA

ICSA-23-068-04: **Step Tools Third-Party**

Low level vulnerability: Null Pointer Dereference.

Step Tools Third-Party | CISA

ICSA-23-068-02: **B&R Systems Diagnostics Manager**

Medium level vulnerability: Cross-site Scripting.

B&R Systems Diagnostics Manager | CISA

ICSA-23-068-03: **ABB Ability Symphony Plus**

High level vulnerability: Improper Authentication.

ABB Ability Symphony Plus | CISA

ICSA-23-068-01: **Akuvox E11**

Critical level vulnerabilities: Generation of Predictable IV with CBC, User of Hard-coded Cryptographic Key, Missing Authentication for Critical Function, Storing Passwords in a Recoverable Format, Weak Password Recovery Mechanism for Forgotten Password, Command Injection, Reliance on File Name or Extension of Externally-Supplied File, Missing Authorization, Improper Access Control, Exposure of Sensitive Information to an Unauthorized Actor, Improper Authentication, Use of hard-coded Credentials, Hidden Functionality.

Akuvox E11 | CISA

ICSA-23-061-01: **Mitsubishi Electric MELSEC iQ-F Series**

High level vulnerability: Plaintext Storage of a Password.

Mitsubishi Electric MELSEC iQ-F Series | CISA

ICSA-23-061-02: **Baicells Nova**

Critical level vulnerability: Command injection.

Baicells Nova | CISA

ICSA-23-061-03: **Rittal CMC III Access systems**

Low level vulnerability: Improper Access Control.

Rittal CMC III Access systems | 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 Releases Decider Tool to Help with MITRE ATT&CK Mapping

CISA released Decider, a free tool to help the cybersecurity community map threat actor behavior to the MITRE ATT&CK framework. Created in partnership with the Homeland Security Systems Engineering and Development Institute™ (HSSEDI) and MITRE, Decider helps make mapping quick and accurate through guided questions, a powerful search and filter function, and a cart functionality that lets users export results to commonly used formats.

Network defenders, analysts, and researchers can see CISA's video, fact sheet, and blog to get started with Decider. CISA encourages the community to use the tool in conjunction with the recently updated Best Practices for MITRE ATT&CK® Mapping guide.

Source and more information:

https://www.cisa.gov/news-events/alerts/2023/03/01/cisa-releases-decider-tool-help-mitre-attck-mapping