2023 May, 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

ISACA Ransomware Incident Management (Quick Reference)

ISACA published a preparedness checklist, which can help different organizations (including the industrial sector) to handle a Ransomware incident.

Ransomware is an especially egregious form of malware that restricts access to a system and can, at best, temporarily impact revenue generation or, at worst, cause a massive financial loss event that triggers bankruptcy or liquidation. To make things more complicated, the public sector's reliance is growing on private sector entities to defend against ransomware, which has significantly increased the criticality of supply chain risk management.

There are a number of variables that influence an organization's ability to prepare for and recover from a ransomware attack. Your organization can use this checklist in case of a ransomware incident. The quick reference shows the different aspects of a ransomware handling process and is very useful for the SMEs and also for multinational organizations.

Source and more information available on the following link:

https://www.isaca.org/resources/infographics/ransomware-incident-management

ICS trainings, education

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

OT Cybersecurity Summit

This brand-new event will focus on the leading international standards and conformance systems that are being used to keep operational technology (OT) safe and secure in industries such as energy, manufacturing, building automation, and more. New developments within the ISA/IEC 62443 standards series will be highlighted and technical training and certification programs designed to help you implement the standards into your business operations and workforce will be reviewed. Professionals involved in the security process should attend this event to learn more about workforce development strategies, hardware and software protection practices, and ways to improve infrastructure and data security measures.

Aberdeen, Scotland—Virtually or In person; 1st – 3rd June 2023

More details can be found on the following website:

https://industrialcyber.co/event/ot-cybersecurity-summit/

2023 Industrial Control Systems (ICS) Security Symposium series

Public Safety Canada also periodically hosts a focused information session, including presentations and facilitated discussions, for those unfamiliar with the complexities of ICS security. The objective of this foundational session is to provide new skills to Canadian Critical Infrastructure (CI) personnel including management, senior officials, and anyone working at CI sites where ICS are employed. We encourage those responsible for infrastructure security to attend in order to broaden their knowledge of the impacts and issues facing ICS today. Topics covered in this session include:

- What is ICS?: An Introductory Overview
- Information Technology vs. Operational Technology (IT/OT)
- Where ICS is Found: A Walkthrough of ICS in the Water Sector from Water Source to Faucet
- Case Studies of ICS Cyber Events
- Public Safety Canada Resources Available to the CI Community

Singapore, Online; 7th June 2023

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/index-en.aspx

ManuSec World Summit

ManuSec World Summit Returns Online in June 2023, Uniting Global IT and OT Security Experts Over 24-Hours.

After 2022's successful edition, the ManuSec World Summit returns for another year in 2023, bringing together 100's of IT & OT security leaders from major manufacturing organisations, right across the globe.

As a 24-hour virtual event the agenda will follow the path of the sun, starting with expert speakers in the APAC region and transitioning throughout MEA, Europe, LatAm and North America. The summit's dynamic online format allows sponsors, speakers, and attendees to engage and connect through a wide range of interactive sessions and virtual networking opportunities.

This is a unique opportunity for cyber security innovators to build partnerships with senior cyber security professionals across the FMCG, Food & Beverage, Machinery, Automotive, Aerospace, Chemical, Pharma & Transport industries, whilst participating in discussions that are shaping the manufacturing security landscape in 2023 and beyond.

Virtual event; 15th June 2023

More details can be found on the following website:

https://industrialcyber.co/event/manusec-world-24-hour-cyber-security-event/

SANS ICS Europe Summit & Training 2023

SANS continue to deliver relevant cyber security knowledge and skills, empowering students to protect people and their assets. Register for SANS ICS Europe Summit & Training 2023, and continue to build practical cyber security skills you can implement immediately.

Live Online courses include live stream instruction with real-time support from GIAC-certified teacher assistants, plus an archive of course lectures uploaded to your account daily during the event and four months of access to your course lectures recordings.

Munich, DE and Virtual; 19th – 24th June 2023

More details can be found on the following website:

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

ICS incidents

Irrigation Systems in Israel Disrupted by Hacker Attacks on ICS

Hackers targeted water controllers for irrigation systems at farms in the Jordan Valley and wastewater treatment control systems belonging to the Galil Sewage Corporation in a recent attack. The incident highlights how easy it is to hack industrial control systems (ICS) due to a lack of basic security measures such as changing default passwords and not leaving unprotected systems exposed to the internet. The impacted farms likely left their ICS exposed to the internet and used default passwords, enabling hackers to easily gain access and cause disruption. The attacks on water systems in Israel appear to be part of an anti-Israel hacktivist campaign called OpIsrael, which has intensified every year in early April in the past decade. According to reports, authorities worked throughout Sunday morning to resolve the issue and restore the operational status of major systems, but the authorities are still unclear about the identity of the attackers.

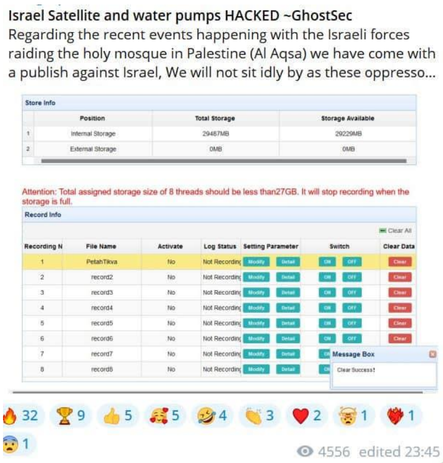
However, as noted by Hackread.com, a group of pro-Palestinian hacktivists going by the online handle of GhostSec took responsibility for cyberattacks on critical infrastructure in Israel. The group claimed it had hacked Israeli satellites and water pumps. Yet, it is unclear if GhostSec hackers are involved in the cyberattacks reported in this article.*

The sources are available on the following links:

https://www.securityweek.com/irrigation-systems-in-israel-disrupted-by-hacker-attacks-on-ics/

* https://www.hackread.com/israel-cyberattacks-hit-critical-infrastructure/

https://www.jpost.com/israel-news/article-738790



Israel Satellite and water pumps HACKED ~GhostSec
Regarding the recent events happening with the Israeli forces raiding the holy mosque in Palestine (Al Aqsa) we have come with a publish against Israel, We will not sit idly by as these oppresso...

Store Info

	Position	Total Storage	Storage Available
1	Internal Storage	29467MB	29229MB
2	External Storage	0MB	0MB

Attention: Total assigned storage size of 8 threads should be less than27GB. It will stop recording when the storage is full.

Record Info

Clear All

Recording N	File Name	Activate	Log Status	Setting Parameter	Switch	Clear Data
1	PetahTikva	No	Not Recording	Modify Detail	ON OFF	Clear
2	record2	No	Not Recording	Modify Detail	ON OFF	Clear
3	record3	No	Not Recording	Modify Detail	ON OFF	Clear
4	record4	No	Not Recording	Modify Detail	ON OFF	Clear
5	record5	No	Not Recording	Modify Detail	ON OFF	Clear
6	record6	No	Not Recording	Modify Detail	ON OFF	Clear
7	record7	No	Not Recording	Modify Detail	ON	
8	record8	No	Not Recording	Modify Detail	ON	

Message Box
Clear Success!

Source *

Book recommendation

Framework for SCADA Cybersecurity

Purpose: Provide Critical Infrastructure customers and academic students an understanding of the NIST Cybersecurity Critical Infrastructure Framework and how to apply the framework to new and existing SCADA applications and implementations.

The objectives of this book are as follows:

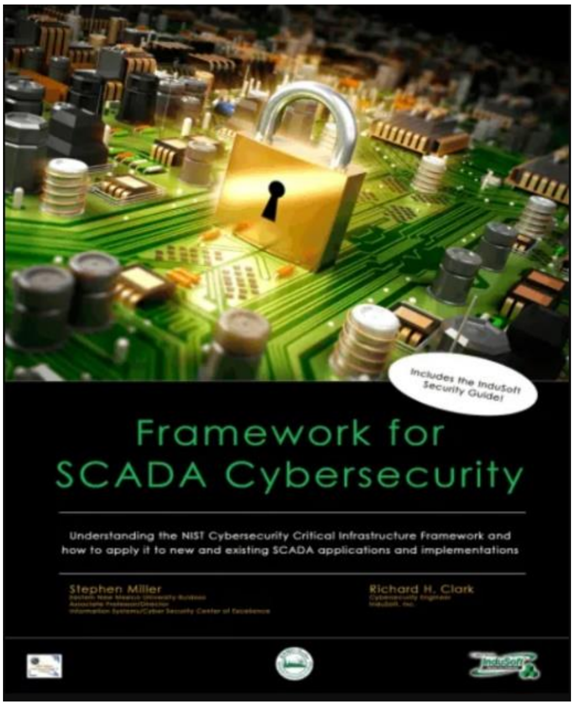
1. Establish an overview and introduction of the EO13636 Improving Critical Infrastructure Cybersecurity.
2. Provide knowledge, understanding, and application of the five functions of the framework.
3. Apply tools and standards to enable the framework implementation.
4. Apply industry security recommendations to meet the framework categories.

Authors/Editors: Richard Clark and Stephen Miller

Year of issue: 2015

The book is available at the following link:

https://www.scribd.com/book/253546236/Framework-for-SCADA-Cybersecurity


Includes the InduSoft Security Guide!
Framework for SCADA Cybersecurity
Understanding the NIST Cybersecurity Critical Infrastructure Framework and how to apply it to new and existing SCADA applications and implementations
Stephen Miller
Eastern New Mexico University-Ruidoso
Associate Professor/Director
Information Systems/Cyber Security Center of Excellence
Richard H. Clark
Cybersecurity Engineer
InduSoft, Inc.
InduSoft

ICS security news selection

Evaluating ICS cyber threat landscape focusing on insider threats in OT environments

Operational technology (OT) environments face numerous cybersecurity risks and threats, such as supply chain security threats, nation-state hackers, malware, ransomware, and ransomware-as-a-service (RaaS) attacks, and data breaches, which can potentially disrupt services and halt production lines. Another key risk that these installations face, comes from the amount of access and control employees and contractors have in these environments, which could enable insider threats to inflict severe collateral damage or potential loss of life, rendering traditional preventative security measures often ineffective.

As external attackers are not the only threats modern organizations need to consider in their cybersecurity planning. Malicious, negligent, and compromised users are also serious and growing risks that organizations must prepare for. Insider threats present a complex and dynamic risk affecting the public and private domains across critical infrastructure sectors. …

Source, and more information:

https://industrialcyber.co/features/evaluating-ics-cyber-threat-landscape-focusing-on-insider-threats-in-ot-environments/

Critical Siemens RTU Vulnerability Could Allow Hackers to Destabilize Power Grid

A critical vulnerability affecting some of Siemens' industrial control systems (ICS) designed for the energy sector could allow malicious hackers to destabilize a power grid, according to the researchers who found the security hole.

The vulnerability, tracked as CVE-2023-28489, impacts the CPCI85 firmware of Sicam A8000 CP-8031 and CP-8050 products, and it can be exploited by an unauthenticated attacker for remote code execution. These products are remote terminal units (RTUs) designed for telecontrol and automation in the energy supply sector, particularly for substations. Patches are available …

Source, and more information:

https://www.securityweek.com/critical-siemens-rtu-vulnerability-could-allow-hackers-to-destabilize-power-grid/

The essence of OT security: A proactive guide to achieving CISA's Cybersecurity Performance Goals

The widespread adoption of remote and hybrid working practices in recent years has brought numerous benefits to various industries, but has also introduced new cyber threats, particularly in the critical infrastructure sector.

These threats extend not only to IT networks but also to operational technology (OT) and cyber-physical systems, which can directly influence crucial physical processes.

In response to these risks, the US government reinforced critical infrastructure security by introducing Cross-Sector Cybersecurity Performance Goals (CPGs) mandated by the US Cybersecurity Infrastructure & Security Agency (CISA).

Recently, CISA updated the CPGs to align with NIST's standard cybersecurity framework, establishing each of the five goals as a prioritized subset of IT and OT cybersecurity practices.

In this article, we will look in more detail at CISA's revamped CPGs and discuss the potential solutions available to help organizations achieve these critical goals. ...

Source, and more information:

https://www.helpnetsecurity.com/2023/05/25/cisa-cybersecurity-performance-goals/

New Russian-linked CosmicEnergy malware targets industrial systems

Mandiant security researchers have discovered a new malware called CosmicEnergy designed to disrupt industrial systems and linked to Russian cybersecurity outfit Rostelecom-Solar (formerly Solar Security).

The malware specifically targets IEC-104-compliant remote terminal units (RTUs) commonly used in electric transmission and distribution operations across Europe, the Middle East, and Asia.

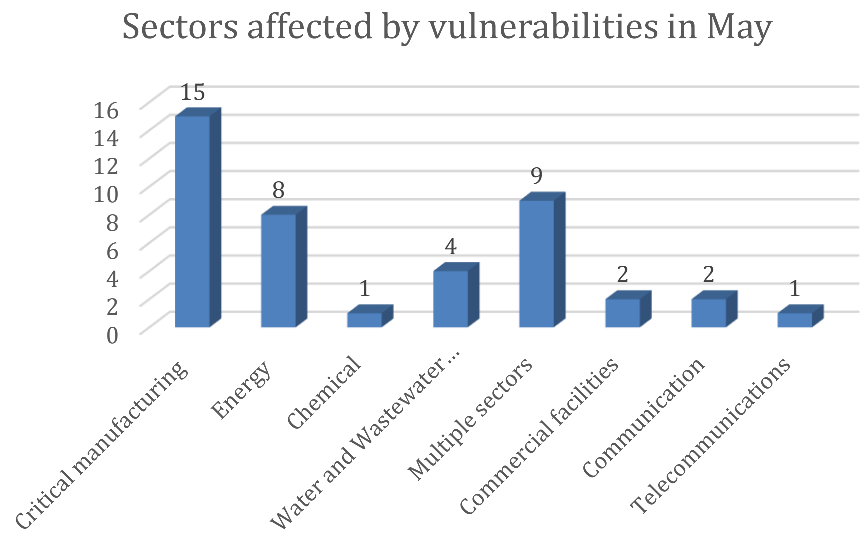
CosmicEnergy was discovered after a sample was uploaded to the VirusTotal malware analysis platform in December 2021 by someone with a Russian IP address. ...

Source, and more information:

https://www.bleepingcomputer.com/news/security/new-russian-linked-cosmicenergy-malware-targets-industrial-systems/

ICS vulnerabilities

In May 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:

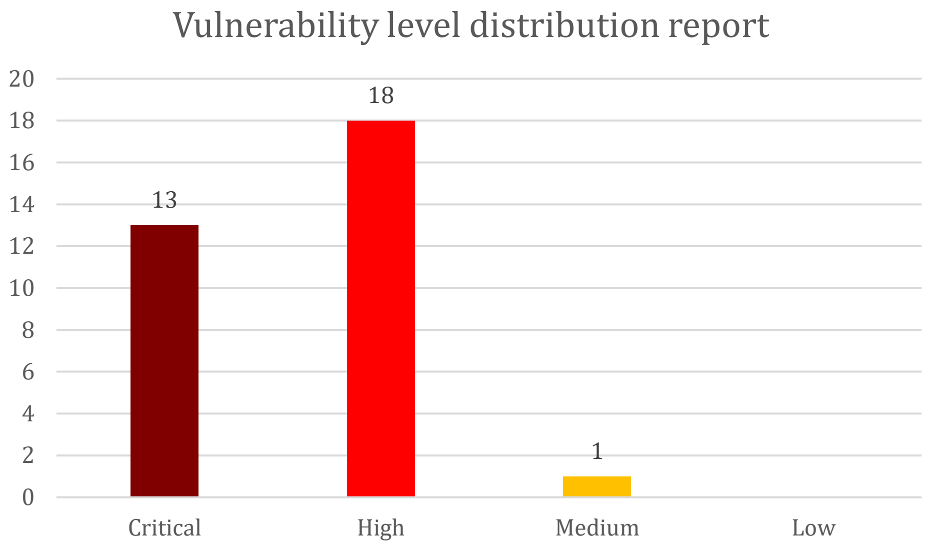


Average number of vulnerabilities per vulnerability report in May: **2,93**

Vulnerabilities/Exploitable remotely: **32/25**

The most common vulnerabilities in May:

Vulnerability	CWE number	Items
Path Traversal	CWE-22	5
Improper Input Validation	CWE-20	4
Out-of-bounds Read	CWE-125	4
Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE-119	4
Exposure of Sensitive Information to an Unauthorized Actor	CWE-200	4



ICSA-23-150-01: **Advantech WebAccess/SCADA**

High level vulnerability: Insufficient Type Distinction.

Advantech WebAccess/SCADA | CISA

ICSA-23-145-01: **Moxa MXsecurity Series**

Critical level vulnerabilities: Command Injection and Use of Hard-Coded Credentials.

Moxa MXsecurity Series | CISA

ICSA-23-143-04: **Horner Automation Cscape**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read, Use After Free, Access of Uninitialized Pointer, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Horner Automation Cscape | CISA

ICSA-23-143-03: **Mitsubishi Electric MELSEC Series CPU module**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric MELSEC Series CPU module | CISA

ICSA-23-143-02: **Hitachi Energy's RTU500 Series Product**

Critical level vulnerabilities: Type Confusion, Observable Timing Discrepancy, Out-of-bounds Read, Infinite Loop, Classic Buffer Overflow.

Hitachi Energy's RTU500 Series Product | CISA

ICSA-23-143-01: **Hitachi Energy’s AFS65x, AFS67x, AFR67x and AFF66x Products**

High level vulnerability: Use After Free.

Hitachi Energy’s AFS65x, AFS67x, AFR67x and AFF66x Products | CISA

ICSA-20-051-02: **Rockwell Automation FactoryTalk Diagnostics (Update B)**

Critical level vulnerability: Deserialization of Untrusted Data.

Rockwell Automation FactoryTalk Diagnostics (Update B) | CISA

ICSA-23-138-04: **Johnson Controls OpenBlue Enterprise Manager Data Collector**

Critical level vulnerabilities: Improper Authentication, Exposure of Sensitive Information to an Unauthorized Actor.

Johnson Controls OpenBlue Enterprise Manager Data Collector | CISA

ICSA-23-138-03: **Hitachi Energy’s MicroSCADA Pro/X SYS600 Products**

Medium level vulnerability: ermissions, Privileges, and Access Controls.

Hitachi Energy’s MicroSCADA Pro/X SYS600 Products | CISA

ICSA-23-138-02: **Mitsubishi Electric MELSEC WS Series**

High level vulnerability: Active Debug Code.

Mitsubishi Electric MELSEC WS Series | CISA

ICSA-23-138-01: **Carlo Gavazzi Powersoft**

High level vulnerability: Path Traversal.

Carlo Gavazzi Powersoft | CISA

ICSA-23-136-03: **Rockwell Automation FactoryTalk Vantagepoint**

High level vulnerability: Insufficient Verification of Data Authenticity.

Rockwell Automation FactoryTalk Vantagepoint | CISA

ICSA-23-136-01: **Snap One OvrC Cloud**

High level vulnerabilities: Improper Input Validation, Observable Response Discrepancy, Improper Access Control, Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity, Open Redirect, Use of Hard-coded Credentials, Hidden Functionality.

Snap One OvrC Cloud | CISA

ICSA-23-136-02: **Rockwell ArmorStart**

High level vulnerability: Improper Input Validation.

Rockwell ArmorStart | CISA

ICSA-23-131-01: **Siemens Solid Edge**

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

Siemens Solid Edge | CISA

ICSA-23-131-02: **Siemens SCALANCE W1750D**

High level vulnerability: Improper Input Validation.

Siemens SCALANCE W1750D | CISA

ICSA-23-131-03: **Siemens Siveillance**

Critical level vulnerability: Deserialization of Untrusted Data.

Siemens Siveillance Video Event and Management Servers | CISA

ICSA-23-131-04: **Siemens SIMATIC Cloud Connect 7**

High level vulnerabilities: Improper Neutralization of Special Elements used in a Command ('Command Injection'), Use of Hard-coded Password, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Missing Standardized Error Handling Mechanism, Exposure of Sensitive Information to an Unauthorized Actor, Files or Directories Accessible to External Parties.

Siemens SIMATIC Cloud Connect 7 | CISA

ICSA-23-131-05: **Siemens SINEC NMS Third-Party**

Critical level vulnerabilities: Expected Behavior Violation, Improper Validation of Syntactic Correctness of Input, Stack-based Buffer Overflow, Use After Free, Double Free, Cleartext Transmission of Sensitive Information.

Siemens SINEC NMS Third-Party | CISA

ICSA-23-131-06: **Siemens SCALANCE LPE9403**

Critical level vulnerabilities: Command Injection, Creation of Temporary File with Insecure Permissions, Path Traversal, Heap-based Buffer Overflow.

Siemens SCALANCE LPE9403 | CISA

ICSA-23-131-07: **Sierra Wireless AirVantage**

High level vulnerabilities: Improper Authentication, Exposure of Sensitive Information to an Unauthorized Actor.

Sierra Wireless AirVantage | CISA

ICSA-23-131-08: **Teltonika Remote Management System and RUT Model Routers**

Critical level vulnerabilities: Observable Response Discrepancy, Improper Authentication, Server-Side Request Forgery, Cross-site Scripting, Inclusion of Web Functionality from an Untrusted Source, External Control of System of Configuration Setting, OS Command Injection.

Teltonika Remote Management System and RUT Model Routers | CISA

ICSA-23-131-09: **Rockwell Automation Kinetix 5500 EtherNetIP Servo Drive**

Critical level vulnerability: Improper Access Control.

Rockwell Automation Kinetix 5500 | CISA

ICSA-23-131-10: **Rockwell Automation Arena Simulation Software**

High level vulnerabilities: Incorrect Restriction of Operations within the Bounds of a Memory Buffer.

Rockwell Automation Arena Simulation Software | CISA

ICSA-23-131-11: **BirdDog Cameras & Encoders**

High level vulnerabilities: Cross-Site Request Forgery, Use of Hard-Coded Credentials.

BirdDog Cameras and Encoders | CISA

ICSA-23-131-12: **SDG PnPSCADA**

Critical level vulnerability: SQL Injection.

SDG PnPSCADA | CISA

ICSA-23-131-13: **PTC Vuforia Studio**

High level vulnerabilities: Insufficiently Protected Credentials, Improper Authorization, Unrestricted Upload of File with Dangerous Type, Path Traversal, Cross-site Request Forgery.

PTC Vuforia Studio | CISA

ICSA-23-131-14: **Rockwell PanelView 800**

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

Rockwell Automation PanelView 800 | CISA

ICSA-23-131-15: **Rockwell ThinManager**

High level vulnerability: Inadequate Encryption Strength.

Rockwell Automation ThinManager | CISA

ICSA-23-129-02: **Hitachi Energy MSM**

Critical level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Authentication Bypass by Capture-replay, Code Injection, Improper Restriction of Operations within the Bounds of a Memory Buffer, NULL Pointer Dereference, Insufficient Entropy.

Hitachi Energy MSM | CISA

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

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

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

ICSA-22-263-03: **Dataprobe iBoot-PDU (Update A)**

Critical level vulnerabilities: OS Command Injection, Path Traversal, Exposure of Sensitive Information to an Unauthorized Actor, Improper Access Control, Improper Authorization, Incorrect Authorization, SSRF, Stack-Based Buffer Overflow, Use of Weak Credentials, Plaintext Storage of a Password, Authentication Bypass Using an Alternate Path or Channel.

Dataprobe iBoot-PDU (Update A) | CISA

ICSA-23-122-01: **Mitsubishi Electric Factory Automation Products**

High level vulnerability: Dependency on Vulnerable Third-Party Component.

Mitsubishi Electric Factory Automation Products | 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 published alerts in 2023 May:

CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans

# National Supply Chain Integrity Month # Covered List # Defending Against Software Supply Chain Attacks # Cyber Supply Chain Risk Management # Vulnerability Scanning

Link and more information:

CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans | CISA

CISA Adds Three Known Exploited Vulnerabilities to Catalog

# Known Exploited Vulnerabilities Catalog # Command Injection Vulnerability # Deserialization of Untrusted Data Vulnerability # Oracle WebLogic Server Unspecified Vulnerability

Link and more information:

CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

# Known Exploited Vulnerabilities Catalog # privilege escalation

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA and Partners Disclose Snake Malware Threat From Russian Cyber Actors

# Hunting Russian Intelligence “Snake” Malware #Russia Cyber Threat Overview and Advisories #Russian state-sponsored cyber activity

Link and more information:

CISA and Partners Disclose Snake Malware Threat From Russian Cyber Actors | CISA