2024 June, 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 podcasts

People listen more and more podcasts nowadays. Whether it's for our personal interests or for our professional development, the world of podcasts is a great possibility to be well informed. In this section, we bring together the ICS security podcasts from the previous month.

Dale Peterson

This podcast is named after and made by one of the most famous ICS security expert, Dale Peterson. It's made on Wednesdays on every week and the usual structure contains an opening monologue, interviews with guests and listener questions on topics that are on the leading, or even bleeding edge of OT and ICS security. The podcast is also interactive, so the listeners could ask questions from Dale and the guests.

You can find all of Peterson's podcasts on the below URL.

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

This podcast is discussing major industrial cybersecurity topics and features industry experts covering everything from ransomware through critical infrastructure to supply chain attacks. Tune in to stay on top of the latest cybersecurity trends, threats and tactics. Hosted by Gary Cohen and Tyler Wall.

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

BEERISAC: OT/ICS Security Podcast Playlist

A curated playlist of Operational Technology and ICS Cyber Security related podcast episodes by ICS Security enthusiasts.

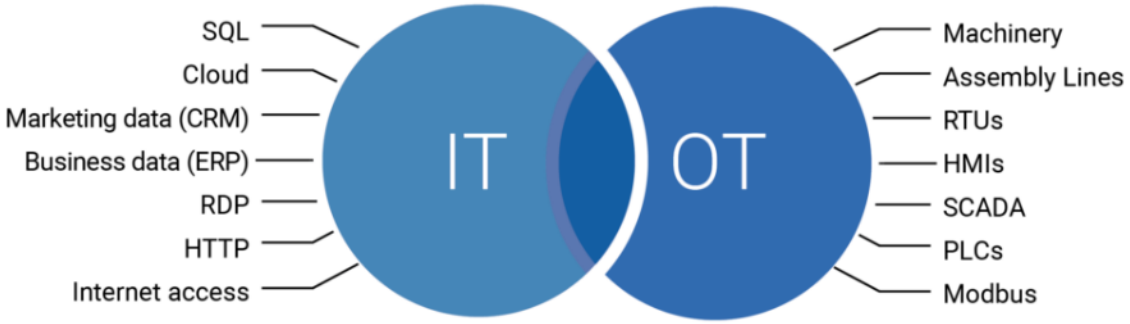
At this link, you can find numerous podcasts on the topic of ICS (Industrial Control Systems) created by various content producers. It's worth browsing through and listening to podcasts that are of interest to the organization or the readers of this newsletter themselves.

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/

ICS good practices, recommendations

Key Strategies and Best Practices for Enhancing OT Security

The publication on the Content Security website highlights the importance of ensuring OT security. The author also illustrates the threat correlations present in IT and OT relationships in the published writing. In addition to mentioning legacy systems and OT protocols, supply chain risks, insider threats, cyber-attacks and the importance of safety is also emphasized. Very important for the understanding the threat landscape:



Implementing best practices is crucial for mitigating risks and ensuring the resilience of OT systems against cyber attacks. Let's delve into some key strategies for enhancing OT cybersecurity:

- Asset inventory and management
- Network segmentation
- Access control and authentication
- Patch management
- Monitoring and logging
- Incident response and recovery
- Employee training and awareness
- Regular risk assessments and audits

The recommendations on how to effectively implement measures to enhance OT security are detailed at the link below.

Source, links and more information available on the following link:

https://contentsecurity.com.au/enhancing-ot-security-strategies/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in July 2024:

- 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/

- 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/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

- NIST(800-82) Industrial Control system(ICS) Security

https://www.udemy.com/course/nist800-82-industrial-control-systemics-security/

- ICS/OT Cybersecurity All in One as per NIST Standards

https://www.udemy.com/course/ics-cybersecurity/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

https://www.infosectrain.com/operational-technology-ot-training-courses/#courses

ICS conferences

In July 2024, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

2024 Chemical Security Seminars

The Cybersecurity and Infrastructure Security Agency (CISA) is hosting the fully virtual 2024 Chemical Security Seminars on July 11 and 18, 2024, from 10 am-3 pm ET (7 am-noon PT). The Seminars are free to attend and open to the public.

The 2024 Seminars will feature important chemical security information for industry organizations, facility owners and operators, government officials, first responders, and law enforcement. Sessions will discuss and share the latest in chemical security best practices, including: Case studies of real-world scenarios, including drones and cyberattacks, Transnational threats to the chemical industry, "Wicked Problems", Updates on CISA's ChemLock program, Artificial intelligence, And more!

Virtual; 11st – 18th July 2024

More details can be found on the following website:

https://www.cisa.gov/news-events/events/2024-chemical-security-seminars

Critical Infrastructure Security Excellence Workshops 2024

The Critical Infrastructure Security Excellence Workshops will include presentations from industry and government representatives on the latest information and practical advice relating to the protection of Australia's critical infrastructure through panel discussions and collaborative activities.

Each workshop will comprise an in-person event, available free of charge for industry professionals, at each capital city around Australia.

Don't miss this opportunity to support the security and resilience uplift of critical infrastructure assets and supply chains. Establish valuable connections with both government and industry representatives.

Perth, Australia; 17th July 2024

More details can be found on the following website:

https://www.cisc.gov.au/how-we-support-industry/events-and-outreach/security-excellence-workshops-2024

18. International Conference on Sustainable Development of Critical Infrastructure

International Conference on Sustainable Development of Critical Infrastructure aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Sustainable Development of Critical Infrastructure. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Sustainable Development of Critical Infrastructure.

London, United Kingdom; 29th – 30th July 2024

More details can be found on the following website:

https://waset.org/sustainable-development-of-critical-infrastructure-conference-in-july-2024-in-london?utm_source=conferenceindex&utm_medium=referral&utm_campaign=listing

ICS incidents

Synnovis Ransomware Attack

On early June, a ransomware attack targeted Synnovis, a pathology services provider, significantly impacting several major NHS hospitals in London. The attack has been attributed to the Qilin ransomware group, a Russian cybercriminal gang, according to Ciaran Martin, the former CEO of the UK's National Cyber Security Centre (NCSC).

The attack has locked Synnovis out of its systems, causing ongoing service disruptions at Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Foundation Trust, and other primary care providers in southeast London. Due to these disruptions, many non-emergency pathology appointments, blood transfusions, and surgeries have been postponed, canceled, or redirected to other providers.

An alert on Synnovis' customer service portal indicates that data center issues have rendered all systems inaccessible. Hospital officials have described the situation as an "ongoing critical incident" with a "major impact" on their operations and procedures. Despite these challenges, urgent and emergency services such as A&E, urgent care centers, and maternity departments remain operational.

An NHS England cyber incident response team is currently assessing the full extent of the attack and its implications for patient and employee data. While the majority of outpatient services continue to function normally, procedures that rely heavily on pathology services have faced significant disruptions. Blood testing is now being prioritized for the most urgent cases, leading to the cancellation of some phlebotomy appointments.

The Qilin ransomware operation, which surfaced in August 2022 under the name "Agenda" and rebranded as Qilin a month later, has been linked to numerous attacks since its inception. The group has added over 130 companies to its dark web leak site in the past two years, with a notable increase in activity towards the end of 2023.

Qilin's operations involve infiltrating company networks, extracting data, and moving through the victim's systems. After obtaining administrative credentials and collecting sensitive data, the attackers deploy ransomware payloads to encrypt all devices connected to the network. The group then uses the stolen data and encrypted files for double-extortion attacks, demanding ransoms that range from $25,000 to millions of dollars depending on the victim's size.

Qilin's dark web leak site is currently down, though there is no evidence linking this outage to the Synnovis ransomware attack. The attack on Synnovis has highlighted the

significant vulnerabilities within healthcare infrastructure, emphasizing the need for robust cybersecurity measures to protect critical systems and patient data.

In summary, the ransomware attack on Synnovis has caused severe disruptions in healthcare services across several major NHS hospitals in London, underscoring the critical importance of cybersecurity in safeguarding essential medical services.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/qilin-ransomware-gang-linked-to-attack-on-london-hospitals/

Book recommendation

Cyber Security and Critical Infrastructures: Volume II

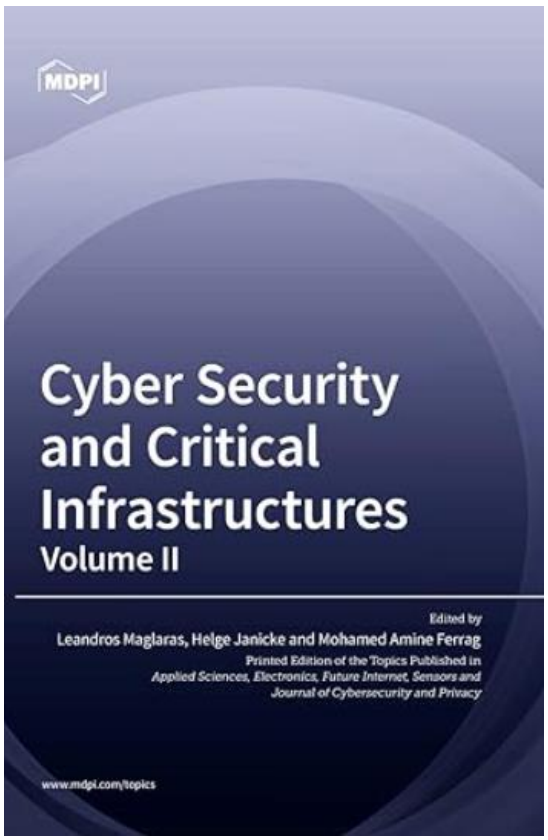
The second volume of the book contains the manuscripts that were accepted for publication in the MDPI Special Topic "Cyber Security and Critical Infrastructure" after a rigorous peer-review process. Authors from academia, government and industry contributed their innovative solutions, consistent with the interdisciplinary nature of cybersecurity. The book contains 16 articles, including an editorial that explains the current challenges, innovative solutions and real-world experiences that include critical infrastructure and 15 original papers that present state-of-the-art innovative solutions to attacks on critical systems.

Author/Editor: Leandros Maglaras (Editor), Helge Janicke (Editor), Mohamed Amine Ferrag (Editor)

Year of issue: 2022

The book is available at the following link:

Cyber Security and Critical Infrastructures: Volume II: Maglaras, Leandros, Janicke, Helge, Ferrag, Mohamed Amine: 9783036556611: Amazon.com: Books



ICS security news selection

Microsoft Warns of Surge in Cyber Attacks Targeting Internet-Exposed OT Devices

Microsoft has emphasized the need for securing internet-exposed operational technology (OT) devices following a spate of cyber attacks targeting such environments since late 2023.

"These repeated attacks against OT devices emphasize the crucial need to improve the security posture of OT devices and prevent critical systems from becoming easy targets," the Microsoft Threat Intelligence team said.

The company noted that a cyber attack on an OT system could allow malicious actors to tamper with critical parameters used in industrial processes, either programmatically via the programmable logic controller (PLC) or using the graphical controls of the human-machine interface (HMI), resulting in malfunctions and system outages. …

Source and more information:

https://thehackernews.com/2024/05/microsoft-warns-of-surge-in-cyber.html

New Kaspersky ICS CERT report reviews Q1 APT, financial attacks on industrial enterprises

New findings by the Kaspersky ICS CERT team offer a comprehensive overview of reported APT (advanced persistent threat) and financial attacks on industrial enterprises from the first quarter of this year. The report also details the activities of groups observed targeting industrial organizations and critical infrastructure facilities. As always, social engineering (phishing) and exploitation of vulnerable internet-facing devices were the most common methods used to penetrate a target organization. …

Source and more information:

https://industrialcyber.co/industrial-cyber-attacks/new-kaspersky-ics-cert-report-reviews-q1-apt-financial-attacks-on-industrial-enterprises/?_gl=1*kt5z1*_up*MQ..*_ga*MjEwMDIwMDE5NS4xNzE4MTE3MTM5*_ga_T2BXH1VHY7*MTcxODExNzEzNy4xLjAuMTcxODExNzEzNy4wLjAuMA..

Forescout identifies PLCs, DCSs, industrial robots as top vulnerabilities in 2024 risk report

Forescout Technologies has found that the most vulnerable OT devices are critical and insecure-by-design PLCs (programmable logic controllers) and DCSs (distributed control systems), with industrial robots emerging as a new risk area. In its fourth annual review conducted by its research division, Vedere Labs, which analyses data from nearly 19 million devices to identify vulnerabilities and threats to critical infrastructure, Forescout also noted that UPSs (Uninterruptible Power Supply) in many data centers still use default credentials. Additionally, building automation systems, commonly overlooked, pose significant security risks. …

Source and more information:

https://industrialcyber.co/threat-landscape/forescout-identifies-plcs-dcss-industrial-robots-as-top-vulnerabilities-in-2024-risk-report/?_gl=1*1hcl1i3*_up*MQ..*_ga*MTk1MjAyNjYxOS4xNzE4MTE3Mjgy*_ga_T2BXH1VHY7*MTcxODExNzI4MS4xLjAuMTcxODExNzI4MS4wLjAuMA..

Rockwell's ICS Directive Comes as Critical Infrastructure Risk Peaks

Critical infrastructure is facing increasingly disruptive threats to physical processes, while thousands of devices are online with weak authentication and riddled with exploitable bugs.

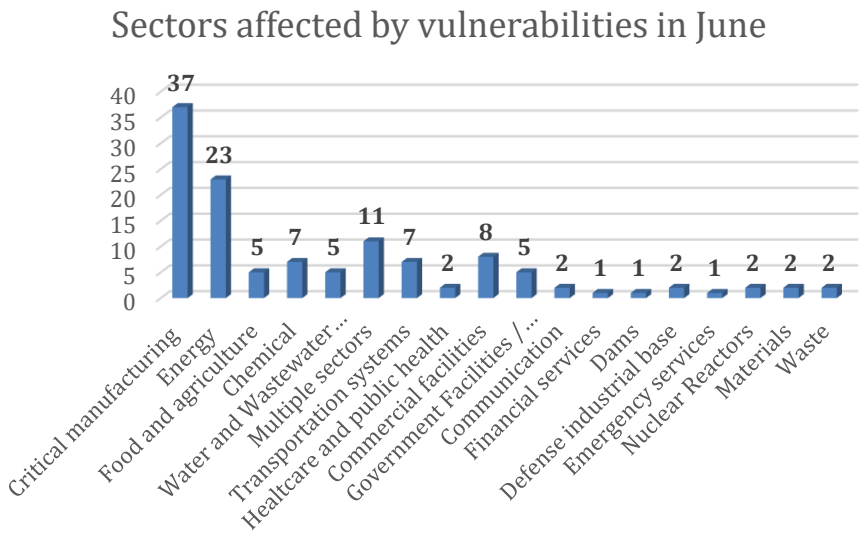
Citing "heightened geopolitical tensions and adversarial cyber activity globally," industrial control systems (ICS) giant Rockwell Automation last month took the unusual step of telling its customers to disconnect their gear from the Internet. The move showcases not just growing cyber risk to critical infrastructure, but the unique challenges that security teams face in the sector, experts say. …

Source and more information:

https://www.darkreading.com/ics-ot-security/rockwell-ics-directive-critical-infrastructure-risk-peaks

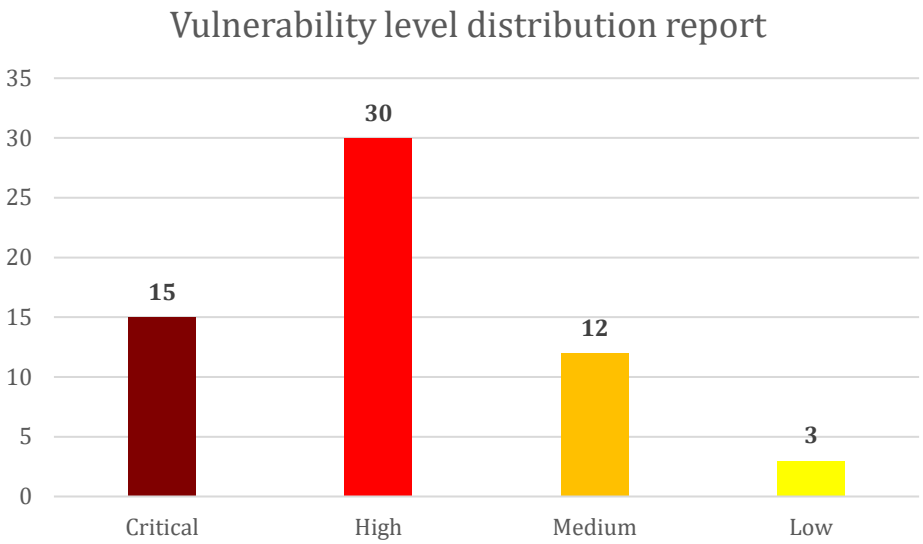
ICS vulnerabilities

In June 2024, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT and Siemens ProductCERT and Siemens CERT:



The most common vulnerabilities in June:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	7
Out-of-bounds Write	CWE-787	6
Integer Overflow or Wraparound	CWE-190	5
Allocation of Resources Without Limits or Throttling	CWE-770	5
NULL Pointer Dereference	CWE-476	5



ICSA-24-179-01: **TELSAT marKoni FM Transmitter**

Critical level vulnerabilities: Command Injection, Use of Hard-coded Credentials, Use of Client-Side Authentication, Improper Access Control.

TELSAT marKoni FM Transmitter | CISA

ICSA-24-179-02: **SDG Technologies PnPSCADA**

Critical level vulnerability: Missing Authorization.

SDG Technologies PnPSCADA | CISA

ICSA-24-179-03: **Yokogawa FAST/TOOLS and CI Server**

Medium level vulnerabilities: Cross-site Scripting, Empty Password in Configuration File.

Yokogawa FAST/TOOLS and CI Server | CISA

ICSA-24-179-04: **Johnson Controls Illustra Essentials Gen 4**

Critical level vulnerability: Improper Input Validation.

Johnson Controls Illustra Essentials Gen 4 | CISA

ICSA-24-179-05: **Johnson Controls Illustra Essentials Gen 4**

Medium level vulnerability: Storing Passwords in a Recoverable Format.

Johnson Controls Illustra Essentials Gen 4 | CISA

ICSA-24-179-06: **Johnson Controls Illustra Essentials Gen 4**

Medium level vulnerability: Insertion of Sensitive Information into Log File.

Johnson Controls Illustra Essentials Gen 4 | CISA

ICSA-24-179-07: **Johnson Controls Illustra Essentials Gen 4**

Medium level vulnerability: Storing Passwords in a Recoverable Format.

Johnson Controls Illustra Essentials Gen 4 | CISA

ICSA-24-177-01: **ABB Ability System 800xA**

Medium level vulnerability: Improper Input Validation.

ABB Ability System 800xA | CISA

ICSA-24-177-02: **PTC Creo Elements/Direct License Server**

Critical level vulnerability: Missing Authorization.

PTC Creo Elements/Direct License Server | CISA

ICSA-24-172-01: **Yokogawa CENTUM**

High level vulnerability: Uncontrolled Search Path Element.

Yokogawa CENTUM | CISA

ICSA-24-172-02: **CAREL Boss-Mini**

Critical level vulnerability: Path Traversal.

CAREL Boss-Mini | CISA

ICSA-24-172-03: **Westermo L210-F2G**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Control of Interaction Frequency.

Westermo L210-F2G | CISA

ICSA-24-170-01: **RAD Data Communications SecFlow-2**

High level vulnerability: Path Traversal.

RAD Data Communications SecFlow-2 | CISA

ICSA-24-165-01: **Siemens Mendix Applications**

High level vulnerability: Improper Privilege Management.

Siemens Mendix Applications | CISA

ICSA-24-165-02: **Siemens SIMATIC S7-200 SMART Devices**

High level vulnerability: Use of Insufficiently Random Values.

Siemens SIMATIC S7-200 SMART Devices | CISA

ICSA-24-165-03: **Siemens TIA Administrator**

Low level vulnerability: Creation of Temporary File in Directory with Insecure Permissions.

Siemens TIA Administrator | CISA

ICSA-24-165-04: **Siemens ST7 ScadaConnect**

High level vulnerabilities: Integer Overflow or Wraparound, Double Free, Improper Certificate Validation, Inefficient Regular Expression Complexity, Improper Check for Unusual or Exceptional Conditions, Improper Input Validation, NULL Pointer Dereference, Missing Encryption of Sensitive Data, Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Resource Consumption.

Siemens ST7 ScadaConnect | CISA

ICSA-24-165-05: **Siemens SITOP UPS1600**

Medium level vulnerability: Out-of-bounds Write.

Siemens SITOP UPS1600 | CISA

ICSA-24-165-06: **Siemens TIM 1531 IRC**

Medium level vulnerabilities: Improper Input Validation, Out-of-bounds Write, Inadequate Encryption Strength, Double Free, Missing Encryption of Sensitive Data, Incorrect Conversion between Numeric Types, Integer Overflow or Wraparound, Double Free, Race Condition, Use After Free, Improper Locking, Improper Certificate Validation, NULL Pointer Dereference, Infinite Loop.

Siemens TIM 1531 IRC | CISA

ICSA-24-165-07: **Siemens PowerSys**

High level vulnerability: Improper Authentication.

Siemens PowerSys | CISA

ICSA-24-165-08: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: Out-of-bounds Read, Allocation of Resources Without Limits or Throttling, NULL Pointer Dereference.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-165-09: **Siemens SICAM AK3/BC/TM**

High level vulnerability: Improper Null Termination.

Siemens SICAM AK3/BC/TM | CISA

ICSA-24-165-10: **Siemens SIMATIC and SIPLUS**

Critical level vulnerabilities: Inadequate Encryption Strength, Improper Restriction of Operations within the Bounds of a Memory Buffer, Race Condition, Injection, Double Free, Integer Overflow or Wraparound, Improper Locking, NULL Pointer Dereference, Use-After-Free, Improper Input Validation, Improper Certificate Validation, Missing Release of Memory after Effective Lifetime, Out-of-bounds Read, Infinite Loop.

Siemens SIMATIC and SIPLUS | CISA

ICSA-24-165-11: **Siemens SCALANCE XM-400, XR-500**

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

Siemens SCALANCE XM-400, XR-500 | CISA

ICSA-24-165-12: **Siemens SCALANCE W700**

Critical level vulnerabilities: Improper Control of a Resource Through its Lifetime, Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Hard-coded Cryptographic Key, Use of Weak Hash, Injection, Unsynchronized Access to Shared Data in a Multithreaded Context, OS Command Injection.

Siemens SCALANCE W700 | CISA

ICSA-24-165-13: **Siemens SINEC Traffic Analyzer**

High level vulnerabilities: Out-of-bounds Write, Insufficient Session Expiration, Cross-Site Request Forgery (CSRF), Insufficiently Protected Credentials, Exposed Dangerous Method or Function, Cleartext Transmission of Sensitive Information, Sensitive Cookie in HTTPS Session Without 'Secure' Attribute, Improper Input Validation.

Siemens SINEC Traffic Analyzer | CISA

ICSA-24-165-14: **Fuji Electric Tellus Lite V-Simulator**

High level vulnerabilities: Out-of-Bound Write, Stack-based Buffer Overflow.

Fuji Electric Tellus Lite V-Simulator | CISA

ICSA-24-165-16: **Rockwell Automation FactoryTalk View SE**

High level vulnerability: Improper Authentication.

Rockwell Automation FactoryTalk View SE | CISA

ICSA-24-165-17: **Rockwell Automation FactoryTalk View SE**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Rockwell Automation FactoryTalk View SE | CISA

ICSA-24-165-18: **Rockwell Automation FactoryTalk View SE**

High level vulnerability: Improper Authentication.

Rockwell Automation FactoryTalk View SE | CISA

ICSA-24-165-19: **Motorola Solutions Vigilant License Plate Readers**

High level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Cleartext Storage in a File or on Disk, Use of Hard-coded Credentials, Insufficiently Protected Credentials, Missing Encryption of Sensitive Data, Authentication Bypass by Capture-replay.

Motorola Solutions Vigilant License Plate Readers | CISA

ICSA-24-074-14: **Mitsubishi Electric MELSEC-Q/L Series (Update B)**

Critical level vulnerabilities: Incorrect Pointer Scaling, Integer Overflow or Wraparound.

Mitsubishi Electric MELSEC-Q/L Series (Update B) | CISA

ICSA-20-245-01: **Mitsubishi Electric Multiple Products (Update G)**

High level vulnerability: Predictable Exact Value from Previous Values.

Mitsubishi Electric Multiple Products (Update G) | CISA

SSA-871704: **Siemens SICAM Products (Update 1.1.)**

High level vulnerabilities: Improper Null Termination, Improper Neutralization of Special Elements used in a Command ('Command Injection'), Cleartext Storage of Sensitive Information.

SSA-871704 (siemens.com)

SSA-832273: **Siemens RUGGEDCOM APE1808 devices (Update 1.3.)**

Critical level vulnerabilities: Multiple.

SSA-832273 (siemens.com)

SSA-753746: **Siemens SIMATIC Software Products (Update 1.2.)**

High level vulnerability: NULL Pointer Dereference.

SSA-753746 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update 1.9.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-599968: **Siemens Profinet Devices (Update 1.6.)**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

SSA-599968 (siemens.com)

SSA-566905: **Siemens Industrial Products (Update 1.2.)**

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

SSA-566905 (siemens.com)

SSA-482757: **Siemens S7-1500 CPU devices (Update 1.4.)**

Low level vulnerability: Missing Immutable Root of Trust in Hardware.

SSA-482757 (siemens.com)

SSA-446448: **Siemens PROFINET Stack Integrated on Interniche Stack (Update 2.1.)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

SSA-446448 (siemens.com)

SSA-407785: **Siemens Parasolid and Teamcenter Visualization (Update 1.2.)**

High level vulnerabilities: NULL Pointer Dereference, Out-of-bounds Read, Out-of-bounds Write, Allocation of Resources Without Limits or Throttling.

SSA-407785 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 1.6.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-353002: **Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family (Update 1.1.)**

Medium level vulnerabilities: Use of Hard-coded Cryptographic Key, Uncontrolled Resource Consumption.

SSA-353002 (siemens.com)

SSA-093430: **Siemens SIMATIC RTLS Locating Manager before V3.0 (Update 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-093430 (siemens.com)

SSA-035466: **Siemens SICAM PAS/PQS (Update 1.1.)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

SSA-035466 (siemens.com)

ICSA-24-163-01: **Rockwell Automation ControlLogix, GuardLogix, and CompactLogix**

High level vulnerability: Always-Incorrect Control Flow Implementation.

Rockwell Automation ControlLogix, GuardLogix, and CompactLogix | CISA

ICSA-24-163-02: **AVEVA PI Web API**

High level vulnerability: Deserialization of Untrusted Data.

AVEVA PI Web API | CISA

ICSA-24-163-03: **AVEVA PI Asset Framework Client**

High level vulnerability: Deserialization of Untrusted Data.

AVEVA PI Asset Framework Client | CISA

ICSA-24-163-04: **Intrado 911 Emergency Gateway**

Critical level vulnerability: SQL Injection.

Intrado 911 Emergency Gateway | CISA

ICSA-23-108-02: **Schneider Electric APC Easy UPS Online Monitoring Software (Update A)**

Critical level vulnerabilities: OS Command Injection, Missing Authentication for Critical Function.

Schneider Electric APC Easy UPS Online Monitoring Software (Update A) | CISA

ICSMA-24-163-01: **MicroDicom DICOM Viewer**

High level vulnerabilities: Improper Authorization in Handler for Custom URL Scheme, Stack-based Buffer Overflow.

MicroDicom DICOM Viewer | CISA

ICSA-24-158-01: **Emerson PACSystem and Fanuc**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity Insufficiently Protected Credentials, Download of Code Without Integrity Check.

Emerson PACSystem and Fanuc | CISA

ICSA-24-158-02: **Emerson Ovation**

Critical level vulnerabilities: Missing Authentication for Critical Function, Insufficient Verification of Data Authenticity.

Emerson Ovation | CISA

ICSA-24-158-03: **Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch**

Medium level vulnerability: Allocation of Resources Without Limits or Throttling.

Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch | CISA

ICSA-24-158-04: **Johnson Controls Software House iStar Pro Door Controller**

Critical level vulnerability: Missing Authentication for Critical Function.

Johnson Controls Software House iStar Pro Door Controller | CISA

ICSA-24-156-01: **Uniview NVR301-04S2-P4**

Low level vulnerability: Cross-site Scripting.

Uniview NVR301-04S2-P4 | CISA

ICSA-23-278-03: **Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch (Update A)**

Medium level vulnerabilities: Observable Timing Discrepancy, Double Free.

Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch (Update A) | CISA

ICSA-22-172-01: **Mitsubishi Electric MELSEC iQ-R, Q, L Series and MELIPC Series (Update C)**

High level vulnerability: Improper Resource Locking.

Mitsubishi Electric MELSEC iQ-R, Q, L Series and MELIPC Series (Update C) | CISA

ICSA-24-151-02: **Fuji Electric Monitouch V-SFT (Update A)**

High level vulnerabilities: Out-of-Bounds Write, Stack-Based Buffer Overflow, Type Confusion.

Fuji Electric Monitouch V-SFT (Update A) | CISA

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

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

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 2024 June:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2017-3506 Oracle WebLogic Server OS Command Injection Vulnerability;
CVE-2024-4610 ARM Mali GPU Kernel Driver Use-After-Free Vulnerability;
CVE-2024-4577 PHP-CGI OS Command Injection Vulnerability;
CVE-2024-32896 Android Pixel Privilege Escalation Vulnerability;
CVE-2024-26169 Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability;
CVE-2024-4358 Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability;
CVE-2022-24816 GeoSolutionsGroup JAI-EXT Code Injection Vulnerability;
CVE-2022-2586 Linux Kernel Use-After-Free Vulnerability;
CVE-2020-13965 Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA

Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access
Snowflake indicated a recent increase in cyber threat activity targeting customer accounts on its cloud data platform. Snowflake issued a recommendation for users to query for unusual activity and conduct further analysis to prevent unauthorized user access.
Links and more information:
Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access | CISA

Fortinet Releases Security Updates for FortiOS
Fortinet has released security updates to address a vulnerability in FortiOS. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Fortinet Releases Security Updates for FortiOS | CISA

Microsoft Releases June 2024 Security Updates
Microsoft has released security updates to address vulnerabilities in multiple products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:

Microsoft Releases June 2024 Security Updates | CISA

Phone Scammers Impersonating CISA Employees

Impersonation scams are on the rise and often use the names and titles of government employees. The Cybersecurity and Infrastructure Security Agency (CISA) is aware of recent impersonation scammers claiming to represent the agency. As a reminder, CISA staff will never contact you with a request to wire money, cash, cryptocurrency, or use gift cards and will never instruct you to keep the discussion secret.

Links and more information:

Phone Scammers Impersonating CISA Employees | CISA

CISA and Partners Release Guidance for Modern Approaches to Network Access Security

CISA, in partnership with the Federal Bureau of Investigation (FBI), released guidance, Modern Approaches to Network Access Security, along with the following organizations:

- *New Zealand's Government Communications Security Bureau (GCSB);*
- *New Zealand's Computer Emergency Response Team (CERT-NZ); and*
- *The Canadian Centre for Cyber Security (CCCS).*

Links and more information:

CISA and Partners Release Guidance for Modern Approaches to Network Access Security | CISA

CISA Releases Guidance on Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses: (SMBs)

CISA released Barriers to Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses: Identifying Challenges and Opportunities, a detailed report exploring challenges to SSO adoption by small and medium-sized businesses (SMBs). The report also identifies potential ways to overcome these challenges and improve an SMB's level of security.

Links and more information:

CISA Releases Guidance on Single Sign-On (SSO) Adoption for Small and Medium-Sized Businesses: (SMBs) | CISA

Juniper Networks Releases Security Bulletin for Juniper Secure Analytics

Juniper Networks released a security bulletin to address multiple vulnerabilities affecting Juniper Secure Analytics optional applications. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Juniper Networks Releases Security Bulletin for Juniper Secure Analytics | CISA

CISA and Partners Release Guidance for Exploring Memory Safety in Critical Open Source Projects

CISA, in partnership with the Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, and Canadian Cyber Security Center, released Exploring Memory Safety in Critical Open Source Projects. This guidance was crafted to provide organizations with findings on the scale of memory safety risk in selected open source software (OSS).

Links and more information:

CISA and Partners Release Guidance for Exploring Memory Safety in Critical Open Source Projects | CISA

Progress Software Releases Security Bulletin for MOVEit Transfer

Progress Software released a security bulletin to address a vulnerability in MOVEit Transfer. A cyber threat actor could exploit this vulnerability to take control of an affected system.

Links and more information:

Progress Software Releases Security Bulletin for MOVEit Transfer | CISA