2023 December, 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 6
ICS incidents 7
Book recommendation 9
ICS security news selection 10
ICS vulnerabilities 12
ICS alerts 21

ICS good practices, recommendations

Whitepaper: Information security for the medical device industry

With a focus on the medical device industry, this paper provides software developers, hardware developers, and manufacturers with an understanding of the necessity and benefits of cybersecurity preparedness that can be achieved through the implementation of an Information Security Management System (ISMS). The implementation of an ISMS is a foundation for industry certification, which is also a beneficial next step for organizations seeking to strengthen their security posture and marketability. Although an ISMS covers many areas of technology, here the publisher delves into the cybersecurity component of it – an emergent top priority for both business and technology leaders in the healthcare industry.

You will gain an understanding of:

- Why cybersecurity and data privacy have become key foci of information security management.
- Why cybersecurity and data privacy are a growing concern for the medical device industry.
- How interconnectivity of supply chains increases risk.
- How medical device recalls, and healthcare data breaches have impacted organizations.
- How ISO/IEC 27001 certification constructs a framework for enhancing your resilience in the face of cybersecurity threats and data breaches.
- How to obtain an independent ISO/IEC 27001 certification.

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

Spotlight: Whitepaper: Information security for the medical device industry - Cyber Defense Magazine

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in January 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/

- NERC CIP EDUCATION (Hybrid) – Miami, FL **(NEW!)**
  Monday, 22 January 2024 8:00 AM - Friday, 26 January 2024 5:00 PM

https://events.eventzilla.net/e/nerc-cip-education-hybrid--miami-fl-2138615897?resp=on&dateid=2138417950

ICS conferences

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

IEEE CCNC STP-CPS 2024

Cyber-Physical Systems (CPS) integrate computing and communication capabilities with monitoring and control of entities in the physical world. These systems are usually composed of a set of networked agents, including sensors, actuators, control processing units, and communication devices. All the critical infrastructures will also be a part of such a cyber-physical ecosystem to enable smart and connected environments. The tight coupling of Cybersystems with the physical systems brings challenges in terms of stability, security, reliability, robustness, and efficiency. The prevalence of such cyber-physical ecosystems, which is inherent in distributed nature, demands to architect models and propose solutions that can suitably address the above-mentioned challenges. A multitude of CPS devices and applications exist in industrial, transportation, medical, home security, building automation, emergency management, power, and many other systems, which serve critical functions in our lives. Given the popularity of CPS applications, securing them against malicious activities is of utmost importance. Otherwise, malfunctioning and insecure CPS devices and applications can cause enormous damage to individuals, businesses, and nations.

Las Vegas, NV, USA; 06th – 09th January 2024

More details can be found on the following website:

http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=175879&copyownerid=5416

ICS incidents

Ransomware Attack on Slovenian Power Company Holding Slovenske Elektrarne (HSE)

Slovenian power company Holding Slovenske Elektrarne (HSE) fell victim to a ransomware attack that compromised its systems, encrypting files. The incident, occurred last Wednesday, and HSE managed to contain it by Friday, November 24. HSE, Slovenia's largest power generation company, plays a critical role in the country's infrastructure, contributing around 60% to domestic production.

While the cyber-attack did not disrupt power production operations, HSE confirmed that its IT systems and files were affected by the ransomware. Uroš Svete, Director of the Information Security Office, assured the public that the organization promptly notified the National Office for Cyber Incidents and engaged external experts to mitigate the attack.

Although HSE has not yet received a ransom demand, it remains on high alert during the ongoing system cleanup. The company's General Manager, Tomaž Štokelj, and Uroš Svete issued a joint statement, emphasizing that the situation is under control, and they do not expect significant operational disruption or economic damage.

The scope of the impact appears limited to the websites of Šoštanj Thermal Power Plants and the Velenje Coal Mine. Unofficial information suggests that the Rhysida ransomware gang is behind the attack, a group known for high-profile incidents and recently flagged by the FBI and CISA for its techniques.

Rhysida, active since May 2023, has targeted organizations globally, including the Chilean Army, Prospect Medical, and the British Library. Notably, Rhysida gained attention by listing a Chinese state-owned electric power conglomerate on its data leak site, allegedly auctioning stolen data for 50 BTC ($1,840,000). The ransom notes typically include an email address without specifying monetary demands, potentially explaining why HSE has not received a ransom demand at this stage.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/slovenias-largest-power-provider-hse-hit-by-ransomware-attack/

Hacktivists Disrupt Irish Water Utility, Hacking Linked to Political Motivations

In a recent cybersecurity incident, threat actors targeted a small water utility in Ireland, causing a two-day interruption in the water supply. The victim of the attack is a private group water utility serving the Erris area, impacting approximately 180 homeowners.

The cyberattack took place on the Eurotronics water pumping system, affecting the Binghamstown/Drum region. Noel Walsh, a member of the group water scheme, described the moment when the utility was compromised, stating, "Our caretaker went down, and when he got to the pumphouse, up on the screen was a sign 'You have been hacked.' Down with Israel was written on it, and the name of the company that hacked us." Eurotronics, a supplier of equipment to schemes across the country, had its system defaced with an anti-Israel message.

The incident prompted the affected water facility to enhance its security systems, acknowledging the inconvenience caused to the local population. Mr. Walsh emphasized that while larger entities like Irish Water might have greater resources for robust firewalls, the attackers managed to disrupt their systems temporarily.

The WesternPeople website reported that the threat actors behind the cyberattack are politically motivated, selecting the equipment for its Israeli origin. This aligns with a recent trend where Iranian threat actors targeted the Municipal Water Authority of Aliquippa, taking control of a booster station. The attackers, allegedly pro-Hamas, defaced a Unitronics Vision system and declared on their Telegram channel that they had targeted several SCADA systems at Israeli water facilities. They emphasized that any equipment "Made In Israel" is considered a legitimate target.

This incident underscores the increasing intersection of cybersecurity threats with geopolitical motivations, highlighting the need for enhanced security measures to safeguard critical infrastructure globally. The affected water utility's response, including system improvements, reflects the ongoing challenges organizations face in defending against politically motivated cyber threats.

The source is available on the following link:

https://securityaffairs.com/155552/hacktivism/hacktivist-hacked-irish-water-utility.html

Book recommendation

Power System Protection and Relaying 1st Edition

This textbook provides an excellent focus on the advanced topics of the power system protection philosophy and gives exciting analysis methods and a cover of the important applications in the power systems relaying. Each chapter opens with a historical profile or career talk, followed by an introduction that states the chapter objectives and links the chapter to the previous ones, and then the introduction for each chapter. All principles are presented in a lucid, logical, step-by-step approach. As much as possible, the authors avoid wordiness and detail overload that could hide concepts and impede understanding. In each chapter, the authors present some of the solved examples and applications using a computer program.

Toward the end of each chapter, the authors discuss some application aspects of the concepts covered in the chapter using a computer program.

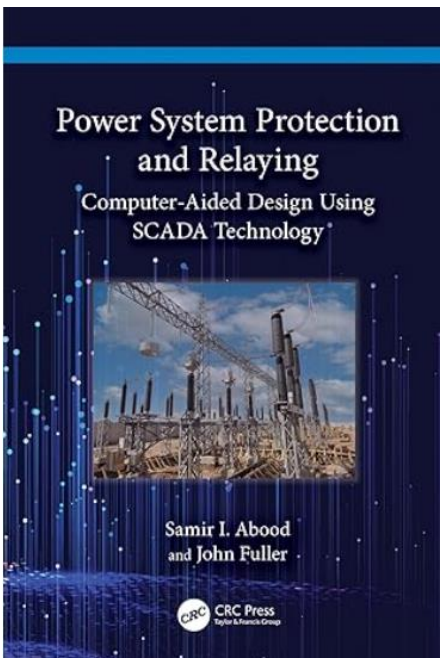
In recognition of requirements by the Accreditation Board for Engineering and Technology (ABET) on integrating computer tools, the use of SCADA technology is encouraged in a student-friendly manner. SCADA technology using the Lucas-Nulle GmbH system is introduced and applied gradually throughout the book.

Author/Editor: Samir I. Abood (Author), John Fuller (Author)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/Power-System-Protection-Relaying-Samir/dp/1032495502



ICS security news selection

Protecting Critical Infrastructure from Cyber Attack

Escalating geopolitical tensions in Europe and Asia place a very big target on western Critical National Infrastructure Industries (CNIs). What better way to attack your enemy than to do so using cyber weapons that are hard to track and even harder to fully attribute to an adversary. Whatsmore, when attribution finally does occur, it is often years later. By that time, the world has usually forgotten and moved on, or has been stunned by an even more destructive cyberattack. Nearly all cyberattacks and cyber-attackers thus far, have gone unpunished. This makes it the perfect crime for perpetrators. …

Source and more information in the free downloadable magazine:

https://cyberdefensemagazine.tradepub.com/free/w_cyba157/

Ransomware Attacks on Industrial Orgs Increasingly Impact OT Systems: Survey

Ransomware attacks aimed at industrial organizations are increasingly impacting operational technology (OT) systems, according to a survey commissioned by OT and IoT security firm Claroty.

Claroty on Wednesday published its 2023 'Global state of industrial cybersecurity' report, which is based on responses from a survey of 1,100 IT and OT security professionals representing organizations in the Americas, EMEA and APAC regions. …

Source and more information:

https://www.securityweek.com/ransomware-attacks-on-industrial-orgs-increasingly-impact-ot-systems-survey/

MITRE Unveils EMB3D Threat Model for Embedded Devices Used in Critical Infrastructure

MITRE has teamed up with the cybersecurity community and the industrial sector to create EMB3D, a threat model specifically designed for embedded devices used in critical infrastructure.

EMB3D is the work of MITRE, Red Balloon Security, Narf Industries, and Niyo 'Little Thunder' Pearson of ONE Gas.

Its goal is to provide a collaborative framework that enables organizations to have a common understanding of the threats targeting embedded devices and how those threats can be mitigated. …

Source and more information:

https://www.securityweek.com/mitre-unveils-emb3d-threat-model-for-embedded-devices-used-in-critical-infrastructure/

Industry regulations and standards are driving OT security priorities

When it comes to ransomware attacks, the impact on OT environments is catching up to the impact on IT environments, according to Claroty.

In Claroty's previous survey conducted in 2021, 32% of ransomware attacks impacted IT only, while 27% impacted both IT and OT. Today, 21% impact IT only, while 37% impact both IT and OT – a significant 10% jump for the latter in just two years.

This trend speaks to the expanding attack surface area and risk of operational disruption that comes with IT/OT convergence.

Source and more information:

https://www.helpnetsecurity.com/2023/12/13/ot-environments-ransomware-impact/

A closer look at the manufacturing threat landscape

The manufacturing industry is embracing digital transformation to fuel efficiency and productivity. However, this evolution is accompanied by profound and growing cybersecurity challenges.

In the linked video, Kory Daniels, CISO at Trustwave, discusses recent comprehensive research highlighting the distinct cybersecurity threats confronting manufacturers.

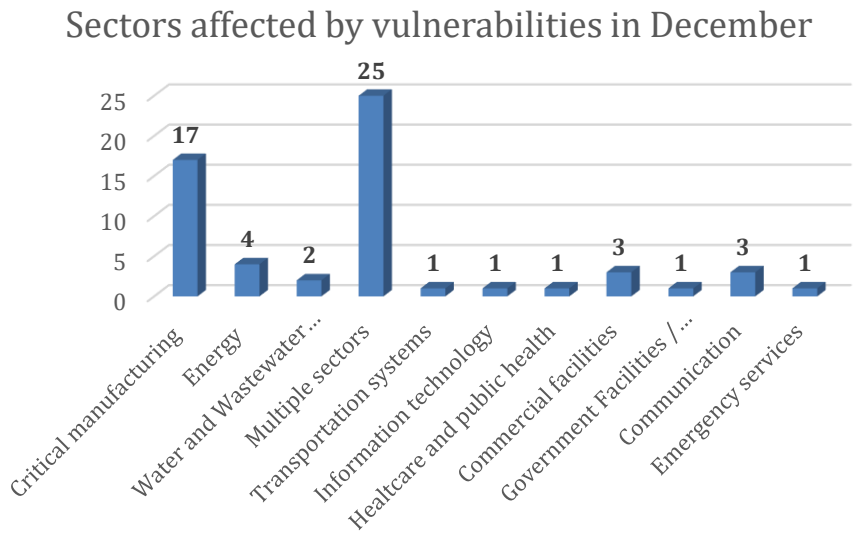
Trustwave SpiderLabs has documented the attack flow utilized by threat groups, exposing their tactics, techniques, and procedures. From email-borne malware to exploiting SMB and DCOM protocols for lateral movement, these persistent threats pose significant risks to the manufacturing sector.

Source, the video and more information:

https://www.helpnetsecurity.com/2023/12/21/manufacturers-threats-video/

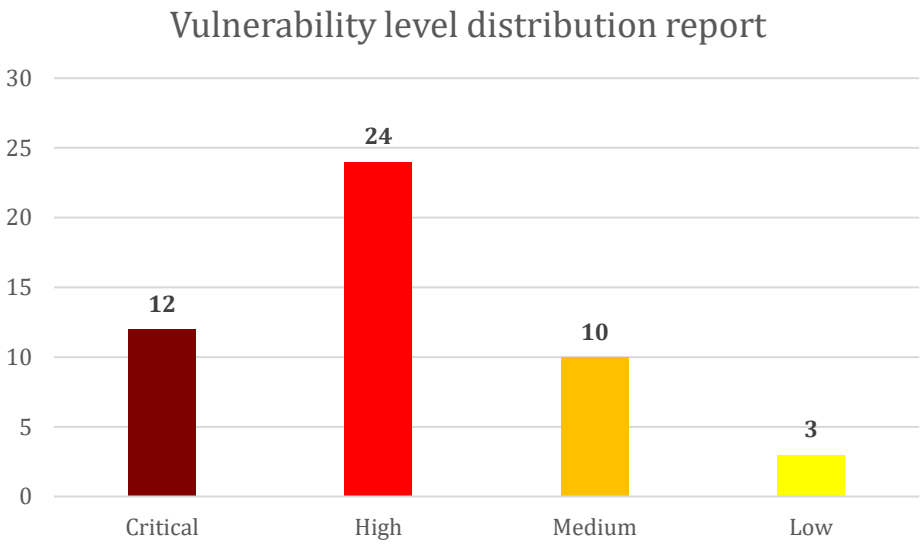
ICS vulnerabilities

In December 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 December:

Vulnerability	CWE number	Items
OS Command Injection	CWE-78	5
Improper Input Validation	CWE-20	5
Cross-site Scripting	CWE-79	5
Uncontrolled Resource Consumption	CWE-400	5



ICSA-23-355-01: **FXC AE1021/AE1021PE**

High level vulnerability: OS Command Injection.

FXC AE1021/AE1021PE | CISA

ICSA-23-355-02: **QNAP VioStor NVR**

High level vulnerability: OS Command Injection.

QNAP VioStor NVR | CISA

ICSA-23-353-01: **Subnet Solutions Inc. PowerSYSTEM Center**

High level vulnerability: Unquoted Search Path or Element.

Subnet Solutions Inc. PowerSYSTEM Center | CISA

ICSA-23-353-02: **EFACEC BCU 500**

Critical level vulnerabilities: Uncontrolled Resource Consumption, Cross-site Request Forgery.

EFACEC BCU 500 | CISA

ICSA-23-353-03: **EFACEC UC 500E**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Open Redirect, Exposure of Sensitive Information to an Unauthorized Actor, Improper Access Control.

EFACEC UC 500E | CISA

ICSA-23-353-04: **Open Design Alliance Drawing SDK**

High level vulnerabilities: Use after Free, Heap-based Buffer Overflow.

Open Design Alliance Drawing SDK | CISA

ICSA-23-353-05: **EuroTel ETL3100 Radio Transmitter**

Critical level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Authorization Bypass Through User-Controlled Key, Improper Access Control.

EuroTel ETL3100 Radio Transmitter | CISA

ICSA-23-341-03: **Johnson Controls Metasys and Facility Explorer (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.

Johnson Controls Metasys and Facility Explorer (Update A) | CISA

ICSA-20-303-01: **Mitsubishi Electric MELSEC iQ-R, Q, and L Series (Update D)**

High level vulnerability: Uncontrolled Resource Consumption.

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

ICSA-23-348-01: **Cambium ePMP 5GHz Force 300-25 Radio**

High level vulnerability: Code Injection.

Cambium ePMP 5GHz Force 300-25 Radio | CISA

ICSA-23-348-02: **Johnson Controls Kantech Gen1 ioSmart**

High level vulnerability: Missing Release of Memory after Effective Lifetime.

Johnson Controls Kantech Gen1 ioSmart | CISA

ICSA-23-348-03: **Siemens User Management Component (UMC)**

High level vulnerabilities: Permissive Cross-domain Policy with Untrusted Domains, Cross-site Scripting, Classic Buffer Overflow, Improper Input Validation.

Siemens User Management Component (UMC) | CISA

ICSA-23-348-04: **Siemens LOGO! and SIPLUS LOGO!**

High level vulnerability: Improper Protection against Electromagnetic Fault Injection (EM-FI).

Siemens LOGO! and SIPLUS LOGO! | CISA

ICSA-23-348-05: **Siemens SIMATIC and SIPLUS Products**

High level vulnerabilities: Uncontrolled Recursion, Buffer Access with Incorrect Length Value.

Siemens SIMATIC and SIPLUS Products | CISA

ICSA-23-348-06: **Siemens OPC UA Implementation in SINUMERIK ONE and SINUMERIK MC**

High level vulnerability: Integer Overflow or Wraparound.

Siemens OPC UA Implementation in SINUMERIK ONE and SINUMERIK MC | CISA

ICSA-23-348-07: **Siemens SIMATIC STEP 7 (TIA Portal)**

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

Siemens SIMATIC STEP 7 (TIA Portal) | CISA

ICSA-23-348-08: **Siemens Web Server of Industrial Products**

High level vulnerability: Missing Release of Memory after Effective Lifetime.

Siemens Web Server of Industrial Products | CISA

ICSA-23-348-09: **Siemens Simantic S7-1500 CPU family**

High level vulnerability: Use After Free.

Siemens Simantic S7-1500 CPU family | CISA

ICSA-23-348-10: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1**

Critical level vulnerabilities: Multiple.

Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 | CISA

ICSA-23-348-11: **Siemens SINUMERIK**

High level vulnerability: Use After Free.

Siemens SINUMERIK | CISA

ICSA-23-348-12: **Siemens SICAM Q100 Devices**

Medium level vulnerabilities: CSRF, Incorrect Permission Assignment for Critical Resource.

Siemens SICAM Q100 Devices | CISA

ICSA-23-348-13: **Siemens SCALANCE and RUGGEDCOM M-800/S615 Family**

High level vulnerabilities: Acceptance of Extraneous Untrusted Data With Trusted Data, OS Command Injection.

Siemens SCALANCE and RUGGEDCOM M-800/S615 Family | CISA

ICSA-23-348-14: **Siemens RUGGEDCOM and SCALANCE M-800/S615 Family**

Critical level vulnerabilities: Improper Validation of Specified Quantity in Input, Use of Hard-coded Cryptographic Key, Use of Weak Hash, Forced Browsing, Uncontrolled Resource Consumption, Unchecked Return Value, Injection, Unsynchronized Access to Shared Data in a Multithreaded Context, OS Command Injection.

Siemens RUGGEDCOM and SCALANCE M-800/S615 Family | CISA

ICSA-23-348-15: **Unitronics VisiLogic**

Critical level vulnerability: Initialization of a Resource with an Insecure Default.

Unitronics Vision Series | CISA

ICSA-23-348-16: **Siemens SINEC INS**

High level vulnerabilities: Improper Certificate Validation, Improper Input Validation, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Unexpected Status Code or Return Value, Missing Report of Error Condition, Improper Check for Unusual or Exceptional Conditions.

Siemens SINEC INS | CISA

ICSMA-20-254-01: **Philips Patient Monitoring Devices (Update C)**

Medium level vulnerabilities: Improper Neutralization of Formula Elements in a CSV File, Cross-site Scripting, Improper Authentication, Improper Check for Certificate Revocation, Improper Handling of Length Parameter Inconsistency, Improper Validation of Syntactic Correctness of Input, Improper Input Validation, Exposure of Resource to Wrong Sphere.

Philips Patient Monitoring Devices (Update C) | CISA

SSA-983300: **Siemens LOGO! Soft Comfort (Update: 1.1.)**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Uncontrolled Search Path Element.

SSA-983300 (siemens.com)

SSA-955858: **Siemens LOGO! 8 BM Devices (Update: 1.1.)**

Critical level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Input Validation, Improper Validation of Specified Index, Position, or Offset in Input.

SSA-955858 (siemens.com)

SSA-831302: **Siemens SIMATIC S7-1500 TM MFP V1.0 (Update: 1.3.)**

Critical level vulnerabilities: Multiple.

SSA-831302 (siemens.com)

SSA-794697: **Siemens SIMATIC S7-1500 TM MFP V1.0 (Update: 1.5.)**

Critical level vulnerabilities: Multiple.

SSA-794697 (siemens.com)

SSA-783481: **Siemens LOGO! 8 BM (Update: 1.1.)**

Medium level vulnerability: Improper Handling of Exceptional Conditions.

SSA-783481 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update: 1.3.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-699386: **Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family before V4.5 (Update: 1.1.)**

Critical level vulnerabilities: Out-of-bounds Read, Inadequate Encryption Strength, Double Free, NULL Pointer Dereference, Allocation of Resources Without Limits or Throttling, Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Hard-coded Cryptographic Key, Use of Weak Hash, Direct Request ('Forced Browsing'), Uncontrolled Resource Consumption, Unchecked Return Value, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Unsynchronized Access to Shared Data in a Multithreaded Context.

SSA-699386 (siemens.com)

SSA-618620: **Siemens RUGGEDCOM ROS Devices (Update: 1.2.)**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Recursion.

SSA-618620 (siemens.com)

SSA-482757: **Siemens S7-1500 CPU devices (Update: 1.3.)**

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

SSA-482757 (siemens.com)

SSB-439005: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP < V3.1 (Update: 5.8.)**

Medium level vulnerabilities: Multiple.

SSB-439005 (siemens.com)

SSA-264815: **Siemens SIMATIC Products (Update: 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-264815 (siemens.com)

SSA-264814: **Siemens SIMATIC Products (Update: 1.3.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-264814 (siemens.com)

SSA-256353: **Siemens RUGGEDCOM ROS (Update: 1.5.)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Observable Timing Discrepancy, Improperly Implemented Security Check for Standard, Heap-based Buffer Overflow, Integer Overflow or Wraparound, Improper Check for Unusual or Exceptional Conditions.

SSA-256353 (siemens.com)

SSA-240541: **Siemens Industrial Products, WIBU Systems CodeMeter (Update: 1.2.)** **Critical** level vulnerability: Heap-based Buffer Overflow.

SSA-240541 (siemens.com)

SSA-042050: **Siemens TIA Portal (Update: 1.1.)**

Medium level vulnerability: Protection Mechanism Failure.

SSA-042050 (siemens.com)

ICSA-23-346-01: **Schneider Electric Easy UPS Online Monitoring Software**

Medium level vulnerability: Path Traversal.

Schneider Electric Easy UPS Online Monitoring Software | CISA

ICSA-22-356-03: **Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series (Update B)**

High level vulnerability: Improper Resource Shutdown or Release.

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

ICSA-23-341-01: **Mitsubishi Electric FA Engineering Software Products**

Medium level vulnerabilities: Processor Optimization Removal or Modification of Security-Critical Code, Observable Discrepancy.

Mitsubishi Electric FA Engineering Software Products | CISA

ICSA-23-341-02: **Schweitzer Engineering Laboratories SEL-411L**

Low level vulnerability: Improper Restriction of Rendered UI Layers or Frames.

Schweitzer Engineering Laboratories SEL-411L | CISA

ICSA-23-341-03: **Johnson Controls Metasys and Facility Explorer**

High level vulnerability: Uncontrolled Resource Consumption.

Johnson Controls Metasys and Facility Explorer | CISA

ICSA-23-341-05: **ControlbyWeb Relay**

High level vulnerability: Cross-Site Scripting.

ControlbyWeb Relay | CISA

ICSA-23-341-06: **Sierra Wireless AirLink with ALEOS firmware**

High level vulnerabilities: Infinite Loop, NULL Pointer Dereference, Cross-site Scripting, Reachable Assertion, Use of Hard-coded Credentials, Use of Hard-coded Cryptographic Key.

Sierra Wireless AirLink with ALEOS firmware | CISA

ICSA-23-339-01 **Zebra ZTC Industrial ZT400 and Desktop GK420d**

Medium level vulnerability: Authentication Bypass Using an Alternate Path or Channel.

Zebra ZTC Industrial ZT400 and ZTC Desktop GK420d | CISA

ICSA-23-208-03 **Mitsubishi Electric CNC Series (Update D)**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric CNC Series (Update D) | 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 December:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-42917 Apple Multiple Products WebKit Memory Corruption Vulnerability;
CVE-2023-42916 Apple Multiple Products WebKit Out-of-Bounds Read Vulnerability;
CVE-2023-33106 Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability;
CVE-2023-33063 Qualcomm Multiple Chipsets Use-After-Free Vulnerability;
CVE-2023-33107 Qualcomm Multiple Chipsets Integer Overflow Vulnerability;
CVE-2022-22071 Qualcomm Multiple Chipsets Use-After-Free Vulnerability;
CVE-2023-41265 Qlik Sense HTTP Tunneling Vulnerability;
CVE-2023-41266 Qlik Sense Path Traversal Vulnerability;
CVE-2023-6448 Unitronics Vision PLC and HMI Insecure Default Password;
CVE-2023-49897 FXC AE1021, AE1021PE OS Command Injection Vulnerability;
CVE-2023-47565 QNAP VioStor NVR OS Command Injection Vulnerability;
Links and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Removes One Known Exploited Vulnerability From Catalog
CVE-2022-28958 DIR-816L Remote Code Execution Vulnerability;
Links and more information:
CISA Removes One Known Exploited Vulnerability From Catalog | CISA

Apple Releases Security Updates for Multiple Products
Apple has released security updates to address vulnerabilities within Safari, macOS Sonoma, iOS, and iPadOS. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
Apple Releases Security Updates for Multiple Products | CISA

CISA and Partners Release Joint Advisory on IRGC-Affiliated Cyber Actors Exploiting PLCs
CISA, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Environmental Protection Agency (EPA), and the Israel National Cyber Directorate (INCD) released a joint Cybersecurity Advisory (CSA) IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors in response to the active exploitation of Unitronics programmable logic controllers (PLCs) in multiple sectors, including U.S. Water and

Wastewater Systems (WWS) facilities, by Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated advanced persistent threat (APT) cyber actors.
Links and more information:
CISA and Partners Release Joint Advisory on IRGC-Affiliated Cyber Actors Exploiting PLCs | CISA

CISA Releases Advisory on Threat Actors Exploiting CVE-2023-26360 Vulnerability in Adobe ColdFusion

CISA released a Cybersecurity Advisory (CSA), Threat Actors Exploit Adobe ColdFusion CVE-2023-26360 for Initial Access to Government Servers, to disseminate known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs). The vulnerability in ColdFusion (CVE-2023-26360) presents as an improper access control issue and exploitation of this CVE can result in arbitrary code execution.
Links and more information:
CISA Releases Advisory on Threat Actors Exploiting CVE-2023-26360 Vulnerability in Adobe ColdFusion | CISA

CISA Releases Joint Guide for Software Manufacturers: The Case for Memory Safe Roadmaps

CISA published The Case for Memory Safe Roadmaps: Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously in collaboration with the following partners:

- *United States National Security Agency*
- *United States Federal Bureau of Investigation*
- *Australian Signals Directorate's Australian Cyber Security Centre*
- *Canadian Centre for Cyber Security*
- *United Kingdom National Cyber Security Centre*
- *New Zealand National Cyber Security Centre*
- *Computer Emergency Response Team New Zealand*

Links and more information:
CISA Releases Joint Guide for Software Manufacturers: The Case for Memory Safe Roadmaps | CISA

CISA and International Partners Release Advisory on Russia-based Threat Actor Group, Star Blizzard

Cybersecurity and Infrastructure Security Agency (CISA)—in coordination with the United Kingdom's National Cyber Security Centre (UK-NCSC), Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian Centre for Cyber

Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), and the U.S. National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cyber Command Cyber National Mission Force (CNMF)—released a joint Cybersecurity Advisory (CSA) Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns.

Links and more information:

CISA and International Partners Release Advisory on Russia-based Threat Actor Group, Star Blizzard | CISA

Atlassian Releases Security Advisories for Multiple Products

Atlassian has released security updates to address vulnerabilities affecting multiple Atlassian products. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Atlassian Releases Security Advisories for Multiple Products | CISA

CISA Releases SCuBA Google Workspace Secure Configuration Baselines for Public Comment

CISA released the draft Secure Cloud Business Applications (SCuBA) Google Workspace (GWS) Secure Configuration Baselines and the associated assessment tool ScubaGoggles for public comment.

Links and more information:

CISA Releases SCuBA Google Workspace Secure Configuration Baselines for Public Comment | CISA

Apple Releases Security Updates for Multiple Products

Apple has released security updates for Safari, iOS and iPadOS, Sonoma, Ventura, and Monterey to address multiple vulnerabilities.

Links and more information:

Apple Releases Security Updates for Multiple Products | CISA

Microsoft Releases Security Updates for Multiple Products

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 Security Updates for Multiple Products | CISA

The Apache Software Foundation Updates Struts 2

The Apache Software Foundation has released security updates to address a vulnerability (CVE-2023-50164) in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system.

Links and more information:

The Apache Software Foundation Updates Struts 2 | CISA

Adobe Releases Security Updates for Multiple Products

Adobe has released security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Adobe Releases Security Updates for Multiple Products | CISA

CISA and Partners Release Advisory on Russian SVR-affiliated Cyber Actors Exploiting CVE-2023-42793

CISA—along with the U.S. Federal Bureau of Investigation (FBI), National Security Agency (NSA), Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK's National Cyber Security Centre (NCSC)—released a joint Cybersecurity Advisory (CSA), Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally.

Links and more information:

CISA and Partners Release Advisory on Russian SVR-affiliated Cyber Actors Exploiting CVE-2023-42793 | CISA

FortiGuard Releases Security Updates for Multiple Products

FortiGuard has released security updates to address vulnerabilities in multiple FortiGuard products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

FortiGuard Releases Security Updates for Multiple Products | CISA

CISA Releases Advisory on Cyber Resilience for the HPH Sector

CISA released a Cybersecurity Advisory, Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment, that details findings from our risk and vulnerability assessments of a Health and Public Health (HPH) Sector organization.

Links and more information:
CISA Releases Advisory on Cyber Resilience for the HPH Sector | CISA

CISA Secure by Design Alert Urges Manufacturers to Eliminate Default Passwords
CISA published guidance on How Manufacturers Can Protect Customers by Eliminating Default Passwords as a part of our new Secure by Design (SbD) Alert series.
Links and more information:
CISA Secure by Design Alert Urges Manufacturers to Eliminate Default Passwords | CISA

FBI, CISA, and ASD's ACSC Release Advisory on Play Ransomware
Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Play Ransomware, to disseminate Play ransomware group's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as October 2023.
Links and more information:
FBI, CISA, and ASD's ACSC Release Advisory on Play Ransomware | CISA

CISA and FBI Release Advisory on ALPHV Blackcat Affiliates
CISA and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), #StopRansomware: ALPHV Blackcat, to disseminate known ALPHV Blackcat affiliates' tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as Dec. 6, 2023. The advisory also provides updates to the FBI FLASH BlackCat/ALPHV Ransomware Indicators of Compromise released April 19, 2022.
Links and more information:
CISA and FBI Release Advisory on ALPHV Blackcat Affiliates | CISA

Mozilla Releases Security Updates for Firefox and Thunderbird
Mozilla has released security updates to address vulnerabilities in Firefox and Thunderbird. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Mozilla Releases Security Updates for Firefox and Thunderbird | CISA

Apple Releases Security Updates for Multiple Products

Apple has released security updates to address vulnerabilities in Safari, iOS, iPadOS, and macOS Sonoma. A cyber threat actor could exploit one of these vulnerabilities to obtain sensitive information.

Links and more information:

Apple Releases Security Updates for Multiple Products | CISA

CISA Releases Microsoft 365 Secure Configuration Baselines and SCuBAGear Tool

CISA has published the finalized Microsoft 365 Secure Configuration Baselines, designed to bolster the security and resilience of organizations' Microsoft 365 (M365) cloud services.

Links and more information:

CISA Releases Microsoft 365 Secure Configuration Baselines and SCuBAGear Tool | CISA