2024 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, podcasts, 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 question 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

Enhancing Security Collaboration Between IT & OT Teams

The issue of collaboration and security between IT and OT systems is not a new challenge. However, it remains a critical topic for organizations operating ICS (Industrial Control Systems). An e-book from 2022 explores this subject in detail. It is recommended that organizations review the insights provided in this publication!

Most industrial organizations experience a lack of security collaboration between IT–SOC analysts and operational teams.

To help ensure business continuity and operational resilience, industrial IT and OT teams should collaborate effectively together, rather than in a siloed manner.

Download the eBook from the linked website to take a deeper dive into the challenges, benefits and need for IT and OT teams to work in close collaboration.

Source and more information available on the following link:

https://www.ot.today/whitepapers/enhancing-security-collaboration-between-ot-teams-w-11247?rf=RAM_Resources

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in January 2025:

- 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

- OT Railway Cybersecurity (OTCS)

https://informaconnect.com/ot-railway-cybersecurity-otcs/

!NEW! in this ICS security feed:

- OT Security Expert (*Master OT/ICS security essentials for protecting critical infrastructure in the digital era*)

https://opswatacademy.com/courses/ot-security-expert

- CTR-008 - OT-Security Awareness E-Learning Course

https://www.yokogawa.com/eu/solutions/products-and-services/trainings-und-workshops/kompetenztrainings/ctr-008-ot-security-awareness-e-learning-course/

ICS conferences

In January 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

The 9th International Conference on Robotics, Control and Automation

The conference aims to boost development of the robotics, control and automation field, expand channels of international academic exchange in science and technology, build a sharing platform of academic resources, promote scientific innovation on the global scale. It also aims to encourage exchange of information on research frontiers in different fields, turn research results into industrial solutions, bring together talents, technologies and capital to boost development. ICRCA will be a perfect gathering to learn about new perspectives, technologies and trends which might pushes the boundaries of the technology and eventually creates a broader future for applications.

Shanghai, China; 10th – 12th January 2025

More details can be found on the following website:

https://www.icrca.org/index.html

CS4CA MENA

This event is returning to the MENA region in the context of being the world's most targeted regions for cyber-attacks, largely due to the region's rapid level of growth combined with pre-existing political tensions. In addition to that, OT environments continue to converge with IT networks, making it more critical than ever to secure these technologies to support continuous uptime and safety.

Dubai, UAE; 21st – 22nd January 2025

More details can be found on the following website:

https://mena.cs4ca.com/

ICS incidents

Energy Sector Contractor ENGlobal Targeted in Ransomware Attack

ENGlobal Corporation, a contractor in the energy sector based in Houston, Texas, reported a ransomware attack that impacted its operations. The attack was discovered on November 25, prompting the company to take immediate containment measures by disconnecting certain systems to prevent further damage. An investigation revealed that a threat actor had infiltrated the company's IT systems and encrypted some of its data files.

Upon identifying the breach, ENGlobal engaged cybersecurity specialists, restricted access to its IT systems, and launched an internal investigation. The company is currently working on recovery efforts but has not provided a timeline for when full access to its IT systems will be restored. As a precautionary step, only essential business operations remain accessible.

ENGlobal has not disclosed whether any data was exfiltrated during the incident or provided details about the ransomware used in the attack. Additionally, no ransomware groups have claimed responsibility for the breach as of now.

The company has also informed the U.S. Securities and Exchange Commission (SEC) about the attack but is unsure whether the incident will have a significant financial or operational impact. ENGlobal specializes in providing engineering and professional services, particularly automated control systems for energy, government, and commercial sectors, and the disruption underscores the vulnerability of critical infrastructure service providers to cyberattacks.

This incident highlights the ongoing cybersecurity challenges faced by organizations in the energy sector, which are increasingly targeted by ransomware operators due to the critical nature of their operations.

The source is available on the following link:

https://www.securityweek.com/energy-sector-contractor-englobal-targeted-in-ransomware-attack/

Romanian energy supplier Electrica hit by ransomware attack

The Electrica Group, a major Romanian electricity distributor and supplier serving over 3.8 million customers, is currently dealing with a ransomware attack. The company confirmed that the attack is under investigation in collaboration with national cybersecurity authorities and that its critical systems have not been compromised. To safeguard its infrastructure, Electrica has implemented temporary protective measures, which may cause minor disruptions in customer interactions. The company’s primary focus remains on maintaining electricity distribution and securing personal and operational data.

Despite the ransomware attack, Electrica's SCADA systems, crucial for monitoring and controlling the electricity distribution network, were not impacted. According to Energy Minister Sebastian Burduja, the SCADA infrastructure remains fully operational and insulated from the affected network equipment. Technical teams and cybersecurity partners are actively working to mitigate risks and ensure the continuity of services.

The ransomware incident follows a series of cyber-related disruptions in Romania, including over 85,000 cyberattacks targeting the country’s election infrastructure in November 2024. This broader context of heightened cybersecurity threats emphasizes the importance of robust security measures for critical infrastructure operators like Electrica.

Electrica's proactive approach, including isolating affected systems and collaborating with cybersecurity agencies, highlights the company's commitment to maintaining service reliability and protecting sensitive data. However, the attack underscores ongoing challenges in securing critical infrastructure, particularly in the energy sector.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/romanian-energy-supplier-electrica-hit-by-ransomware-attack/

Book recommendation

Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats?: Part 1. Secure ICS Architecture

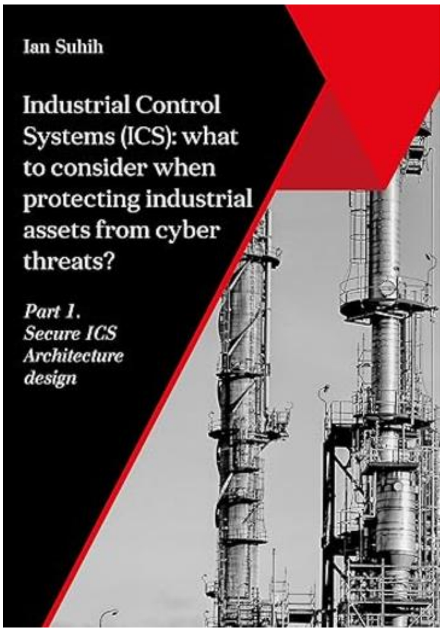
Currently, the international cybersecurity environment is tense. While until recently, cyber threats were considered primarily in relation to the theft of confidential information and extortion, governments are now increasingly talking about cyber weapons and the possibility of physical damage to critical infrastructure. This can be achieved by attacking industrial control systems (ICS) that connect the world of information technology and real industrial processes. Traditionally, systems of this class were poorly protected from cyber-threats, or not protected at all, which now puts entire industries at risk. This paper discusses practical issues of ICS protection and in particular, issues related to the design of secure ICS architectures.

Author/Editor: Ian Suhih (Author)

Year of issue: 2021

The book is available at the following link:

https://www.amazon.com/Industrial-Control-Systems-ICS-Architecture-ebook/dp/B08YD8HRPR



Ian Suhih

Industrial Control Systems (ICS): what to consider when protecting industrial assets from cyber threats?

Part 1. Secure ICS Architecture design

ICS security news selection

Harnessing Smart Digital Reality and Twinning for Next-generation Cyber Risk Mitigation

In today’s rapidly evolving digital landscape, the challenges surrounding cybersecurity are growing exponentially. Industrial sectors, including energy, manufacturing, and utilities, are increasingly becoming targets for cyber threats, particularly as their reliance on Operational Technology (OT) and Industrial Control Systems (ICS) expands. As cyber threats become more sophisticated, traditional approaches to cybersecurity are proving insufficient to safeguard these critical infrastructures. …

Source and more information:

Cyber Defense eMagazine December 2024

IT OT Convergence Insights Report 2024

The IT OT Convergence Insights Report 2024 is part of IoT Analytics’ ongoing coverage of Industrial IoT. The information presented in this report is based on the results of secondary research and qualitative research, i.e., interviews with multiple stakeholders from the IT and OT domain between December 2023 and September 2024. The document includes the definition of IT-OT convergence, drivers and challenges of IT-OT convergence, 27 unique convergence themes grouped into seven categories, and more than 70 corresponding examples of IT-OT convergence implementation. …

Source and more information:

IT OT Convergence Insights Report 2024

Vulnerability Management Challenges in IoT & OT Environments

As Internet of Things (IoT) andoperational technology (OT) devices proliferate across critical infrastructure, manufacturing, healthcare, and other sectors, they bring with them unique and significant security challenges. These devices are increasingly woven into the fabric of everyday business operations, making them essential, yet difficult to secure. While vulnerability management is a well-understood practice in traditional IT environments, IoT and OT introduce complexities that render many of these traditional practices less effective, if not completely obsolete. Here are some of the key challenges, along with strategies for tackling them. …

Source and more information:

https://www.darkreading.com/vulnerabilities-threats/vulnerability-management-challenges-iot-ot-environments

DHS, DTRA lead maritime cybersecurity exercise in Philippines, boost Indo-Pacific security efforts

The U.S. Department of Homeland Security (DHS), in collaboration with the Defense Threat Reduction Agency (DTRA) and U.S. Embassy Manila, conducted last week a high-impact maritime cybersecurity tabletop exercise and chemical security workshop with the Government of the Philippines. The exercise tested realistic scenarios involving sophisticated cyberattacks on critical port infrastructure, including automated cargo handling systems and communication networks. Participants evaluated the effectiveness of their existing emergency procedures, coordination mechanisms, information-sharing agreements, and communications plans. …

Source and more information:

https://industrialcyber.co/training/dhs-dtra-lead-maritime-cybersecurity-exercise-in-philippines-boost-indo-pacific-security-efforts/

Iran-linked IOCONTROL malware targets critical IoT/OT infrastructure in Israel, US

Researchers from Claroty's Team82 arm have obtained a sample of a custom-built IoT/OT malware called IOCONTROL used by the Iran-affiliated attackers to attack Israel- and U.S.-based OT/IoT devices. IOCONTROL has been used to attack IoT and SCADA/OT (supervisory control and data acquisition/operational technology) devices of various types including IP cameras, routers, PLCs (programmable logic controllers), HMIs (human-machine interfaces), firewalls, and other similar devices. Some of the affected vendors include Baicells, D-Link, Hikvision, Red Lion, Orpak, Phoenix Contact, Teltonika, Unitronics, and others. …

Source and more information:

https://industrialcyber.co/news/iran-linked-iocontrol-malware-targets-critical-iot-ot-infrastructure-in-israel-us/

Researchers reveal OT-specific malware in use and in development

Malware that's made specifically to target industrial control systems (ICS), Internet of Things (IoT) and operational technology (OT) control devices is still rare, but in the last few weeks security researchers have identified two salient threats based on samples uploaded to VirusTotal:

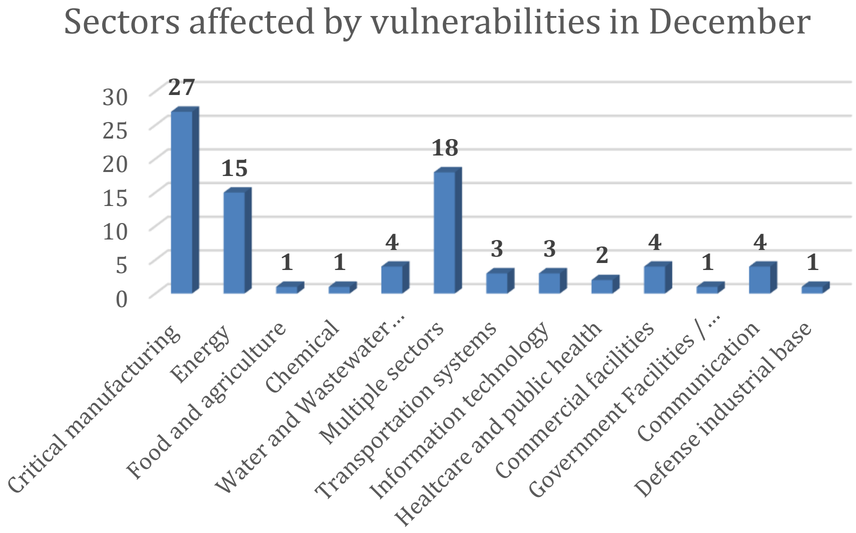
- Claroty's Team82 researchers have unearthed IOCONTROL, a piece of malware that appears to be generic enough to run on a variety of platforms and devices from different vendors.
- Forescout's Vedere Labs researchers have pinpointed a piece of malware they dubbed Chaya_003, which is apparently aimed at engineering workstations running Siemens TIA Portal software. …

Source and more information:

https://www.helpnetsecurity.com/2024/12/17/ot-specific-malware-siemens-industrial-iot/

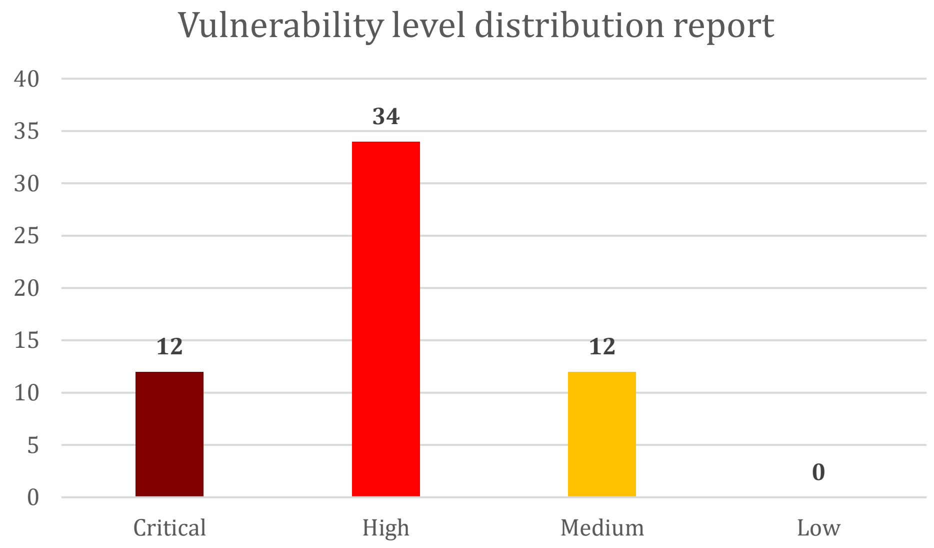
ICS vulnerabilities

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
Out-of-bounds Write	CWE-787	7
Improper Input Validation	CWE-20	7
Out-of-bounds Read	CWE-125	5
Cross-site Scripting	CWE-79	5



ICSA-24-354-01: **Hitachi Energy RTU500 series CMU**

Medium level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

Hitachi Energy RTU500 series CMU | CISA

ICSA-24-354-02: **Hitachi Energy SDM600**

High level vulnerabilities: Origin Validation Error, Incorrect Authorization.

Hitachi Energy SDM600 | CISA

ICSA-24-354-03: **Delta Electronics DTM Soft**

High level vulnerability: Deserialization of Untrusted Data.

Delta Electronics DTM Soft | CISA

ICSA-24-354-04: **Siemens User Management Component**

Critical level vulnerability: Heap-based Buffer Overflow.

Siemens User Management Component | CISA

ICSA-24-354-05: **Tibbo AggreGate Network Manager**

High level vulnerability: Unrestricted Upload of File with Dangerous Type.

Tibbo AggreGate Network Manager | CISA

ICSA-24-354-06: **Schneider Electric Accutech Manager**

High level vulnerability: Classic Buffer Overflow.

Schneider Electric Accutech Manager | CISA

ICSA-24-354-07: **Schneider Electric Modicon Controllers**

Medium level vulnerability: Cross-site Scripting.

Schneider Electric Modicon Controllers | CISA

ICSA-24-352-01: **ThreatQuotient ThreatQ Platform**

High level vulnerability: Command Injection.

ThreatQuotient ThreatQ Platform | CISA

ICSA-24-352-02: **Hitachi Energy TropOS Devices Series 1400/2400/6400**

Medium level vulnerability: Improper Input Validation.

Hitachi Energy TropOS Devices Series 1400/2400/6400 | CISA

ICSA-24-352-03: **Rockwell Automation PowerMonitor 1000 Remote**

Critical level vulnerabilities: Unprotected Alternate Channel, Heap-based Buffer Overflow, Classic Buffer Overflow.

Rockwell Automation PowerMonitor 1000 Remote | CISA

ICSA-24-352-04: **Schneider Electric Modicon**

Critical level vulnerability: Improper Input Validation.

Schneider Electric Modicon | CISA

ICSMA-24-352-01: **BD Diagnostic Solutions Products**

High level vulnerability: Use of Default Credentials.

BD Diagnostic Solutions Products | CISA

ICSA-24-347-01: **Siemens CPCI85 Central Processing/Communication**

Medium level vulnerability: Insufficiently Protected Credentials.

Siemens CPCI85 Central Processing/Communication | CISA

ICSA-24-347-02: **Siemens Engineering Platforms**

High level vulnerability: Improper Input Validation.

Siemens Engineering Platforms | CISA

ICSA-24-347-03: **Siemens RUGGEDCOM ROX II**

High level vulnerability: Cross-Site Request Forgery.

Siemens RUGGEDCOM ROX II | CISA

ICSA-24-347-04: **Siemens Parasolid**

High level vulnerability: Out-of-bounds Write.

Siemens Parasolid | CISA

ICSA-24-347-05: **Siemens Engineering Platforms**

High level vulnerability: Deserialization of Untrusted Data.

Siemens Engineering Platforms | CISA

ICSA-24-347-06: **Siemens Simcenter Femap**

High level vulnerabilities: Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Simcenter Femap | CISA

ICSA-24-347-07: **Siemens Solid Edge SE2024**

High level vulnerabilities: Heap-based Buffer Overflow, Integer Underflow (Wrap or Wraparound).

Siemens Solid Edge SE2024 | CISA

ICSA-24-347-08: **Siemens COMOS**

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

Siemens COMOS | CISA

ICSA-24-347-09: **Siemens Teamcenter Visualization**

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

Siemens Teamcenter Visualization | CISA

ICSA-24-347-10: **Siemens SENTRON Powercenter 1000**

Medium level vulnerability: Incorrect Synchronization.

Siemens SENTRON Powercenter 1000 | CISA

SSA-981975: **Siemens SIMATIC IPCs (Update 1.4.)**

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

SSA-981975

SSA-962515: **Siemens Industrial Products (Update 1.5.)**

High level vulnerability: Out-of-bounds Read.

SSA-962515

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update 1.2.)**

Medium level vulnerability: URL Redirection to Untrusted Site ('Open Redirect').

SSA-876787

SSA-822518: **Siemens RUGGEDCOM APE1808 Devices (Update 1.2.)**

High level vulnerabilities: Insufficient Control of Network Message Volume (Network Amplification), Exposure of Sensitive System Information to an Unauthorized Control Sphere, External Control of File Name or Path, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Insufficiently Protected Credentials, Externally Controlled Reference to a Resource in Another Sphere, Unrestricted Upload of File with Dangerous Type, Server-Side Request Forgery (SSRF).

SSA-822518

SSA-773256: **Siemens Industrial Products (Update 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-773256

SSA-723487: **Siemens SCALANCE, RUGGEDCOM and Related Products (Update 1.3.)** **Critical** level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-711309: **Siemens SIMATIC Products (Update 2.2.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309

SSA-698820: **Siemens RUGGEDCOM APE1808 Devices (Update 1.4.)**

High level vulnerabilities: Session Fixation, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Missing Authentication for Critical Function, Incorrect Parsing of Numbers with Different Radices, Improperly Implemented Security Check for Standard, Improper Access Control.

SSA-698820

SSA-673996: **Siemens SICAM and SITIPE Products (Update 1.1.)**

High level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

SSA-673996

SSA-599968: **Siemens Profinet Devices (Update 1.8.)**

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

SSA-599968

SSA-583523: **Siemens Tecnomatix Plant Simulation (Update 1.1.)**

High level vulnerabilities: Multiple.

SSA-583523

SSA-455250: **Siemens RUGGEDCOM APE1808 Devices Before V11.1.2-h3 (Update 1.5.)** **Critical** level vulnerabilities: Multiple.

SSA-455250

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 2.1.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-364175: **Palo Alto Networks Virtual NGFW on RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update 1.4.)**

Critical level vulnerabilities: Truncation of Security-relevant Information, Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Improper Input Validation, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Out-of-bounds Write.

SSA-364175

SSA-340240: **Siemens SENTRON Powercenter 1000/1100 With 3RV2921-5M Accessory (Update 1.1.)**

High level vulnerability: Improper Check for Unusual or Exceptional Conditions.

SSA-340240

SSA-264815: **Siemens SIMATIC Products (Update 1.3.)**

High level vulnerability: Improper Input Validation.

SSA-264815

SSA-264814: **Siemens SIMATIC Products (Update 1.4.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-264814

SSA-097435: **Siemens Mendix Runtime (Update 1.6.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435

SSA-042050: **Siemens TIA Portal (Update 1.2.)**

Medium level vulnerability: Protection Mechanism Failure.

SSA-042050

ICSA-24-345-01: **MOBATIME Network Master Clock**

Critical level vulnerability: Use of Default Credentials.

MOBATIME Network Master Clock | CISA

ICSA-24-345-02: **Schneider Electric EcoStruxure Foxboro DCS Core Control Services**

High level vulnerabilities: Out-of-bounds Write, Improper Validation of Array Index, Improper Input Validation.

Schneider Electric EcoStruxure Foxboro DCS Core Control Services | CISA

ICSA-24-345-03: **Schneider Electric FoxRTU Station**

High level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Schneider Electric FoxRTU Station | CISA

ICSA-24-345-04: **National Instruments LabVIEW**

High level vulnerability: Out-of-bounds Read.

National Instruments LabVIEW | CISA

ICSA-24-345-05: **Horner Automation Cscape**

High level vulnerability: Out-of-bounds Read.

Horner Automation Cscape | CISA

ICSA-24-345-06: **Rockwell Automation Arena**

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

Rockwell Automation Arena | CISA

ICSA-24-338-01: **Ruijie Reyee OS (Update A)**

Critical level vulnerabilities: Weak Password Recovery Mechanism for Forgotten Password, Exposure of Private Personal Information to an Unauthorized Actor, Premature Release of Resource During Expected Lifetime, Insecure Storage of Sensitive Information, Use of Weak Credentials, Improper Neutralization of Wildcards or Matching Symbols, Improper Handling of Insufficient Permissions or Privileges, Server-Side Request Forgery (SSRF), Use of Inherently Dangerous Function, Resource Leak.

Ruijie Reyee OS (Update A) | CISA

ICSA-24-340-01: **AutomationDirect C-More EA9 Programming Software**

High level vulnerability: Stack-based Buffer Overflow.

AutomationDirect C-More EA9 Programming Software | CISA

ICSA-24-340-02: **Planet Technology Planet WGS-804HPT**

Critical level vulnerabilities: Stack-based Buffer Overflow, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Integer Underflow (Wrap or Wraparound).

Planet Technology Planet WGS-804HPT | CISA

ICSA-24-338-01: **Ruijie Reyee OS**

Critical level vulnerabilities: Weak Password Recovery Mechanism for Forgotten Password, Exposure of Private Personal Information to an Unauthorized Actor, Premature Release of Resource During Expected Lifetime, Insecure Storage of Sensitive Information, Use of Weak Credentials, Improper Neutralization of Wildcards or Matching Symbols, Improper Handling of Insufficient Permissions or Privileges, Server-Side Request Forgery (SSRF), Use of Inherently Dangerous Function, Resource Leak.

Ruijie Reyee OS | CISA

ICSA-24-338-02: **Siemens RUGGEDCOM APE1808**

Critical level vulnerabilities: Missing Authentication for Critical Function, NULL Pointer Dereference, Improper Limitation of a Pathname to a Restricted Directory

('Path Traversal'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-338-03: **Open Automation Software**

High level vulnerability: Incorrect Execution-Assigned Permissions.

Open Automation Software | CISA

ICSA-24-338-04: **ICONICS and Mitsubishi Electric GENESIS64 Products**

High level vulnerabilities: Uncontrolled Search Path Element, Dead Code.

ICONICS and Mitsubishi Electric GENESIS64 Products | CISA

ICSA-24-338-05: **Fuji Electric Monitouch V-SFT**

High level vulnerability: Out-of-bounds Write.

Fuji Electric Monitouch V-SFT | CISA

ICSA-24-338-06: **Fuji Electric Tellus Lite V-Simulator**

High level vulnerability: Out-of-bounds Write.

Fuji Electric Tellus Lite V-Simulator | CISA

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

Medium level vulnerabilities: Insufficient Verification of Data Authenticity, Path Traversal, Unrestricted Upload of File with Dangerous Type, Cross-site Scripting, Cross-Site Request Forgery, Cleartext Transmission of Sensitive Information.

ETIC Telecom Remote Access Server (RAS) (Update B) | CISA

ICSA-24-184-03: **ICONICS and Mitsubishi Electric Products (Update A)**

High level vulnerabilities: Allocation of Resources Without Limits or Throttling, Improper Verification of Cryptographic Signature, Uncontrolled Search Path Element, Improper Authentication, Unsafe Reflection.

ICONICS and Mitsubishi Electric Products (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 December:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-45727 North Grid Proself Improper Restriction of XML External Entity (XEE) Reference Vulnerability;
CVE-2024-11680 ProjectSend Improper Authentication Vulnerability;
CVE-2024-11667 Zyxel Multiple Firewalls Path Traversal Vulnerability;
CVE-2024-51378 CyberPanel Incorrect Default Permissions Vulnerability;
CVE-2024-49138 Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability;
CVE-2024-50623 Cleo Multiple Products Unrestricted File Upload Vulnerability;
CVE-2024-20767 Adobe ColdFusion Improper Access Control Vulnerability;
CVE-2024-35250 Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability;
CVE-2024-55956 Cleo Multiple Products Unauthenticated File Upload Vulnerability;
CVE-2018-14933 NUUO NVRmini Devices OS Command Injection Vulnerability;
CVE-2022-23227 NUUO NVRmini 2 Devices Missing Authentication Vulnerability;
CVE-2019-11001 Reolink Multiple IP Cameras OS Command Injection Vulnerability;
CVE-2021-40407 Reolink RLC-410W IP Camera OS Command Injection Vulnerability;
CVE-2024-12356 BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability;
CVE-2021-44207 Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability;
CVE-2024-3393 Palo Alto Networks PAN-OS Malformed DNS Packet Vulnerability;
Links and more information:
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers
CISA—in partnership with the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and international partners—released joint guidance, Enhanced Visibility and Hardening Guidance for Communications Infrastructure.

Links and more information:
[CISA and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers | CISA]

CISA Releases New Public Version of CDM Data Model Document
Cybersecurity and Infrastructure Security Agency (CISA) released an updated public version of the Continuous Diagnostics and Mitigation (CDM) Data Model Document. Version 5.0.1 aligns with fiscal year 2023 Federal Information Security Modernization Act (FISMA) metrics.
Links and more information:
CISA Releases New Public Version of CDM Data Model Document | CISA

ASD's ACSC, CISA, and US and International Partners Release Guidance on Choosing Secure and Verifiable Technologies
CISA—in partnership with the Australian Signals Directorate Australian Cyber Security Centre (ASD ACSC), and other international partners—released updates to a Secure by Design Alert, Choosing Secure and Verifiable Technologies.
Links and more information:
ASD's ACSC, CISA, and US and International Partners Release Guidance on Choosing Secure and Verifiable Technologies | CISA

Cisco Releases Security Updates for NX-OS Software
Cisco released security updates to address a vulnerability in Cisco NX-OS software. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Cisco Releases Security Updates for NX-OS Software | CISA

Adobe Releases Security Updates for Multiple Products
Adobe released security updates to address vulnerabilities in multiple Adobe software products including Adobe Acrobat, Adobe Illustrator, and Adobe InDesign. 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

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

Apple Releases Security Updates for Multiple Products

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

Links and more information:

Apple Releases Security Updates for Multiple Products | CISA

CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to WWS Sector

CISA and the Environmental Protection Agency (EPA) released Internet-Exposed HMIs Pose Cybersecurity Risks to Water and Wastewater Systems. This joint fact sheet provides Water and Wastewater Systems (WWS) facilities with recommendations for limiting the exposure of Human Machine Interfaces (HMIs) and securing them against malicious cyber activity.

Links and more information:

CISA and EPA Release Joint Fact Sheet Detailing Risks Internet-Exposed HMIs Pose to WWS Sector | CISA

CISA Requests Public Comment for Draft National Cyber Incident Response Plan Update

CISA—through the Joint Cyber Defense Collaborative and in coordination with the Office of the National Cyber Director (ONCD)—released the National Cyber Incident Response Plan Update Public Comment Draft. The draft requests public comment on the National Cyber Incident Response Plan (NCIRP)—public comment period begins today and concludes on January 15, 2025.

Links and more information:

CISA Requests Public Comment for Draft National Cyber Incident Response Plan Update | CISA

CISA and ONCD Release Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure

CISA and the Office of the National Cyber Director (ONCD) published Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure to assist grant-making agencies to incorporate cybersecurity into their grant programs and assist grant-recipients to build cyber resilience into their grant-funded infrastructure projects.

Links and more information:

CISA and ONCD Release Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure | CISA

CISA Issues BOD 25-01, Implementing Secure Practices for Cloud Services

CISA issued Binding Operational Directive (BOD) 25-01, Implementing Secure Practices for Cloud Services to safeguard federal information and information systems. This

Directive requires federal civilian agencies to identify specific cloud tenants, implement assessment tools, and align cloud environments to CISA's Secure Cloud Business Applications (SCuBA) secure configuration baselines.
Links and more information:
[CISA Issues BOD 25-01, Implementing Secure Practices for Cloud Services | CISA]

CISA Releases Best Practice Guidance for Mobile Communications
CISA released Mobile Communications Best Practice Guidance. The guidance was crafted in response to identified cyber espionage activity by People's Republic of China (PRC) government-affiliated threat actors targeting commercial telecommunications infrastructure, specifically addressing "highly targeted" individuals who are in senior government or senior political positions and likely to possess information of interest to these threat actors.
Links and more information:
[CISA Releases Best Practice Guidance for Mobile Communications | CISA]

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