2024 August, 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

Choosing SCADA Selection Criteria and Guidelines

When choosing SCADA software, there are several factors to consider. An article by Roy Kok highlights the various circumstances that play a role in selecting the right solution. The checklist to consider is as follows:

- Vertical Market Specialization – Has a proven track record as a SCADA solution of choice in your market.
- Code vs No-Code Capability – Offers configurable vs. programmable application development.
- Scalability – Handles both today's and tomorrow's requirements.
- Alarm Management – Offers flexible alarming and supports alarm standards.
- Data Archiving – Contains features for data storage, compression, retrieval, and disk space management.
- User Interface – Delivers a consistent user experience for visualization across various devices and client types, including read-only, interactive, local, and remote.
- Tag Management – Contains options for tag management - Flat Tag Model vs S95 vs UNS (Unified Namespace).
- Data Analytics – Provides tools to develop and manage analytics across real-time and historical domains.
- Report Generation – Provides capability for automated time and event-based reporting.
- Notifications – Offers capacity for email, SMS, and other notification means.
- Rapid Development – Contains time-saving deployment tools to replicate similar functionality – clone and multiply.
- Application Documentation – Contains documentation tools for as-built reporting.
- Workflow Management – Provides tools for managing multi-step processes.
- Recipe Management – Has the ability to set operating parameters based on system requirements.
- IT/OT Integration – Provides tools to read/write, display, and interact with relational databases.
- Trend Analytics – Delivers user tools for history data retrieval and analysis.
- Standards Support – Supports various industry standards (OPC, MQTT, FDA 21 CFR Part 11, ISA95, ISA18.2, etc.).

- Performance Speed & Management – Offers high transaction speed and tools for performance management.
- Reliability – Delivers 24x7x365 solution reliability.
- System Health Monitoring – Provides tools for monitoring operational performance.
- Redundancy – Supports high availability requirements.
- Northbound Protocol Connectivity – Provides client support through one or more standards or proprietary APIs and protocols.
- Southbound Protocol Connectivity – Delivers the required protocol(s) robustly and reliably.
- Flexibility – Contains features and benefits that are differentiators at a detail level.
- Distribution – Is available locally or internationally.
- Interoperability – Plays well with other applications.
- Operating System Support – Is supported on the operating systems important to you.
- Ease of Use – Is designed for user or programmatic configuration.
- Technical Support – Offers quality technical support and various program support types.
- Proven – Should be widely used in the market.
- Vendor Endorsed – Delivers protocol owner endorsement of the solution.
- Certifications – Meets protocol certification requirements.
- Price – Available as a cost competitive solution, especially when considering total cost of ownership (TCO).
- License Model – Offers a license model that fits your OpEx/CapEx budget.

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

https://iconics.com/en-us/Resources/ICONICS-Blog/2024/Choosing-SCADA-Selection-Criteria-and-Guidelines

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in September 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 September 2024, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

OT-ISAC Summit 2024

On its 3rd edition, this year's summit theme, OT Cybersecurity: In The Arms Of AI aims to provide a deeper understanding of AI's transformative impact in the OT/ICS cybersecurity realm, addressing the potential benefits and emerging challenges. Emphasizing the need for collaborative teamwork and boosting talent, we aim to explore innovative ways in which AI can revolutionize cybersecurity measures in OT and ICS, setting new benchmarks in the field.

Singapore, Singapore; 4th – 5th September 2024

More details can be found on the following website:

https://www.otisac.org/otisacsummit2024

Cyber Security for Industrial Control Systems Conference

Industrial Control Systems are constantly exposed to increasingly complex cyber threats. This conference will focus on identifying the latest cybersecurity challenges facing companies today and examine how these can be mitigated against by building resilient and responsive systems. You will also get exclusive insights into new techniques and technologies. Plus, the opportunity to network with some of the UK's cybersecurity giants makes this a must-attend conference for anyone working in critical systems.

London – UK; 12th – 13th September 2024

More details can be found on the following website:

https://www.techuk.org/what-we-deliver/events/cyber-security-for-industrial-control-systems-conference.html

CS4CA Europe

New cyber threats continue to compromise our everyday operations as adversaries have increasingly deployed sophisticated ransomware attacks on our critical systems, exploiting vulnerabilities in our organisations. Consequently, this edition of CS4CA

Europe will focus on the theme of "Ensuring Resilience Through Our IT-OT Architecture in the Face of Evolving Risk". Within just the first six months of 2023, organisations operating critical infrastructure services in the United Kingdom reported more cyberattacks to their operations than any year prior. This was mirrored through the region as 32 percent of all global cyberattacks occurred in Europe in 2023. Although new regulations such as NIS2, The Cyber Resilience Act and Cyber Solidarity Act have been put in place for companies to adopt, few companies continue to have suitable policies in place to prevent, protect and educate their teams. Hence, this need for further knowledge and collaboration is why CS4CA Europe returns to London for its 11th Edition.

London – UK; 24th – 25th September 2024

More details can be found on the following website: https://europe.cs4ca.com/

Industrial IoT and Cybersecurity Conference

Industrial automation has emerged as one of the revolutionary processes for manufacturing companies, after Industry 4.0 came into existence. It peaked post pandemic and became need of the hour for every organization. With digitalization and increase in IT-OT convergence the data and control systems have become vulnerable to cyber threats.

These threats have opened avenues for cybersecurity and cloud security to be applied in the basic working flow of organizations. Altaworld's Industrial IoT & Cybersecurity Conference, scheduled on 24th & 25th September 2024, in Chicago - USA , aims on creating a platform to assemble tech experts from manufacturing firms and technology providers, on assessing the challenges, suffice with the solutions and benchmark the digital strategy.

Chicago - USA; 24th – 25th September 2024

More details can be found on the following website:

https://events.altaworld.tech/industrial-iot-and-cybersecurity-conference.html

Kaspersky Industrial Cybersecurity Conference 2024

Kaspersky Industrial Cybersecurity Conference - is a global conference in the field of industrial cybersecurity, which annually brings together leading information security experts, researchers, industrial automation suppliers, system integrators and

customers from around the world. Kaspersky invites you to take part in a conference dedicated to the study of threats and vulnerabilities in automated process control systems, the use of promising technologies and approaches to the construction of automated process control system information security, industry regulations, as well as real cases of implementation and application of solutions.

Sochi, Russia; 25th – 27th September 2024

More details can be found on the following website:

https://ics.kaspersky.com/conference/

ICS incidents

FrostyGoop ICS Malware Causes Heating Outage in Lviv, Ukraine

In January 2024, a cyberattack using the newly discovered FrostyGoop malware disrupted heating services for 600 apartment buildings in Lviv, Ukraine. This attack, analyzed by industrial cybersecurity firm Dragos, targeted a municipal district energy company and resulted in residents enduring sub-zero temperatures for nearly two days.

In April 2023, attackers accessed the energy facility's systems through a vulnerability in an internet-exposed Mikrotik router. Lack of network segmentation allowed easy access to other systems. By November, hackers had obtained user credentials from the SAM registry hive.

On January 22, 2024, attackers initiated the attack by sending commands via the Modbus protocol to ENCO controllers. They downgraded firmware to disable monitoring and manipulated measurements, causing cold water to be pumped into residential buildings.

FrostyGoop's capability to communicate with ICS devices using the Modbus protocol over port 502 is a notable aspect, as it is the first ICS-specific malware to use Modbus for operational impact. The attackers downgraded controller firmware to prevent operators from monitoring the system accurately, leading to false readings of water temperature.

Russia-linked hackers have previously targeted Ukraine's energy sector, causing power outages in 2015 and 2016. Although Dragos has not attributed this attack to any specific country or threat actor, connections to Moscow-based IP addresses were observed during the January attack. The prevalence of the Modbus protocol in industrial environments poses a significant threat to critical infrastructure across multiple sectors worldwide.

The FrostyGoop malware demonstrates the increasing sophistication of cyberattacks targeting industrial control systems (ICS). The ability to disrupt critical services such as heating underscores the urgent need for improved cybersecurity measures in industrial environments.

The source is available on the following link:

[FrostyGoop ICS Malware Left Ukrainian City's Residents Without Heating - SecurityWeek]

US oil giant confirms cyberattack behind systems shutdown

Halliburton, one of the world's leading providers of services to the energy industry, confirmed that it recently experienced a cyberattack, which forced the company to shut down certain systems. The breach was discovered on August 21, 2024, and was reported in a filing with the U.S. Securities and Exchange Commission (SEC).

Upon learning of the unauthorized access by a third party, Halliburton activated its cybersecurity response plan. The company launched an internal investigation, supported by external advisors, to assess the extent of the breach and take necessary actions to remediate it. As part of their response, Halliburton proactively took several systems offline to protect them and to contain the potential spread of the cyberattack.

Halliburton also notified relevant law enforcement agencies about the incident. The company's IT experts are currently working on restoring the affected systems and evaluating the overall impact of the attack. Despite these efforts, Halliburton has not yet disclosed the exact nature of the cyberattack. A spokesperson for the Department of Energy mentioned that the specifics of the incident are still unknown.

The company has been communicating with its customers and stakeholders regarding the situation. They are following their established safety protocols under the Halliburton Management System to ensure ongoing operations while continuing to assess any effects of the breach.

Halliburton, founded in 1919 and employing over 40,000 people, plays a significant role in the global energy sector. The company reported revenues of $5.8 billion for the second quarter of 2024, with an operating margin of 18%. However, as of the time of reporting, Halliburton had not provided further comments on the situation. This incident recalls past cyberattacks on critical infrastructure, such as the 2021 ransomware attack on Colonial Pipeline, which also led to a systems shutdown.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/us-oil-giant-halliburton-confirms-cyberattack-behind-systems-shutdown/

Book recommendation

Industrial Cyber-Physical Systems

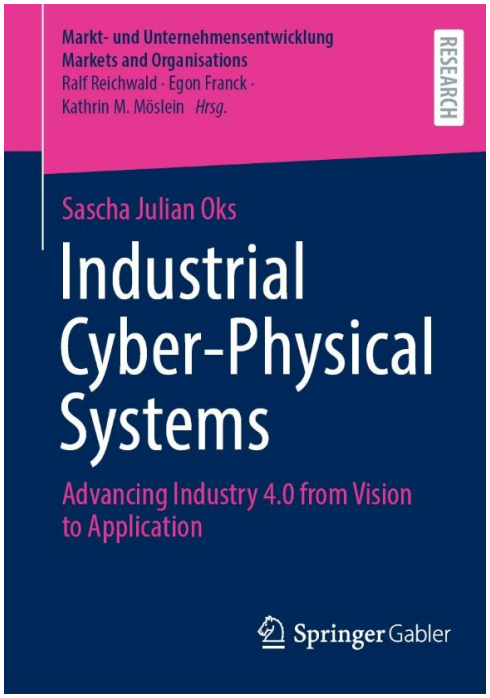
Cyber-physical systems (CPS) are one of the key concepts of Industry 4.0. Despite their great potentials for industrial value creation, there are challenges, such as a significant increase in complexity, as a result of which the development status of Industry 4.0 is behind expectations. This book addresses this issue with the following research design: In addition to providing a comprehensive foundation of industrial CPS and Industry 4.0, four studies are conducted, each consisting of an exploratory research part and a design science research (DSR) part. In doing so, four perspectives are directed at the topic of industrial CPS: A systemic, a stakeholder-centered, an organizational and a holistic. In conclusion, the contributions are integrated in a summary and the artifacts are incorporated into an overarching methodological framework. Thus, theoretical contributions are derived and concrete practical recommendations for the main target groups of organizations, educational institutions and international delegations provided.

Author/Editor: Sascha Julian Oks

Year of issue: 2024

The book is available at the following link:

Industrial Cyber-Physical Systems: Advancing Industry 4.0 from Vision to Application | SpringerLink



ICS security news selection

AI expected to improve IT/OT network management

Once a peripheral concern, OT security has become a mandatory focus for organizations worldwide, according to Cisco's report.

The report provides a comprehensive look at the challenges and opportunities as organizations strive to build a secure and efficient industrial networking foundation. It reflects the global need for robust security solutions specifically designed for the unique needs of industrial environments, and the opportunities for those who can overcome its inherent challenges. …

Source and more information:

https://www.helpnetsecurity.com/2024/08/05/ot-security-posture/

OT Security Is Moving to the Endpoint – Where Humans Interact

When asked why he robbed banks, Depression-era bank robber Willie Sutton purportedly replied, "Because that's where the money is." If Sutton had been a modern-day cybercriminal, the corollary would be, "Why do you attack endpoints? Because that's where humans interact."

In IT security, the biggest threat vectors are social engineering, credential theft and vulnerability exploits. In OT, there are certainly malicious attacks, but many threats involve inadvertent mistakes by employees or authorized third-party technicians who come and go, often remotely. Plant floors are abuzz with activity as internal and external teams work together to keep processes running smoothly. …

Source and more information:

https://industrialcyber.co/expert/ot-security-is-moving-to-the-endpoint-where-humans-interact/

20K Ubiquiti IoT Cameras & Routers Are Sitting Ducks for Hackers

Tens of thousands of small office/home office (SOHO) devices sold by Ubiquiti Inc. are vulnerable on the open Internet to a five-year-old bug, researchers are warning.

In January 2019, broadband Internet expert Jim Troutman warned that an exposed port in dozens of Ubiquiti Internet of Things (IoT) gadgets was being exploited in denial-of-service (DoS) attacks. The underlying vulnerability, CVE-2017-0938, was assigned a "high" 7.5 score on the CVSS scale. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/20k-ubiquiti-iot-cameras-and-routers-are-sitting-ducks-for-hackers

New Forescout-Finite State research exposes security risks in OT, IoT routers with outdated software components

Data from Forescout and Finite State revealed that OT (operational technology) and IoT (Internet of Things) cellular routers, and others used in small offices and homes, have outdated software components that are linked to existing (n-day) vulnerabilities. The Forescout-Finite State report analyzed five firmware images from OT/IoT router vendors including Acksys, Digi, MDEX, Teltonika, and Unitronics, as well as the state of the software supply chain in OT/IoT routers, which are essential for connecting critical devices across various environments to the Internet. The research also found that OT/IoT router firmware images had an average of 20 exploitable n-day vulnerabilities affecting the kernel, with widening security gaps. ...

Source and more information:

https://industrialcyber.co/threat-landscape/new-forescout-finite-state-research-exposes-security-risks-in-ot-iot-routers-with-outdated-software-components/

Rising cybersecurity demands reshape ICS procurement strategies across critical infrastructure

Mounting cybersecurity threats and attacks elevate the priorities of asset owners and operators of critical infrastructure installations to ensure that their supply chains are safe, risk-free, and free from cybersecurity risks in ICS procurement. Vendors shall be expected to provide technological solutions and demonstrate a deep understanding of the application of cybersecurity best practices. This includes implementing robust security measures in their products to protect against adversarial threats targeting OT (operational technology) and ICS (industrial control system) environments, such as malware, ransomware, and nation-state attacks. ...

Source and more information:

https://industrialcyber.co/features/rising-cybersecurity-demands-reshape-ics-procurement-strategies-across-critical-infrastructure/

India's Critical Infrastructure Suffers Spike in Cyberattacks

The financial and government sectors have come under increasing attacks in India, with the Reserve Bank of India (RBI) warning banks to double down on cybersecurity.

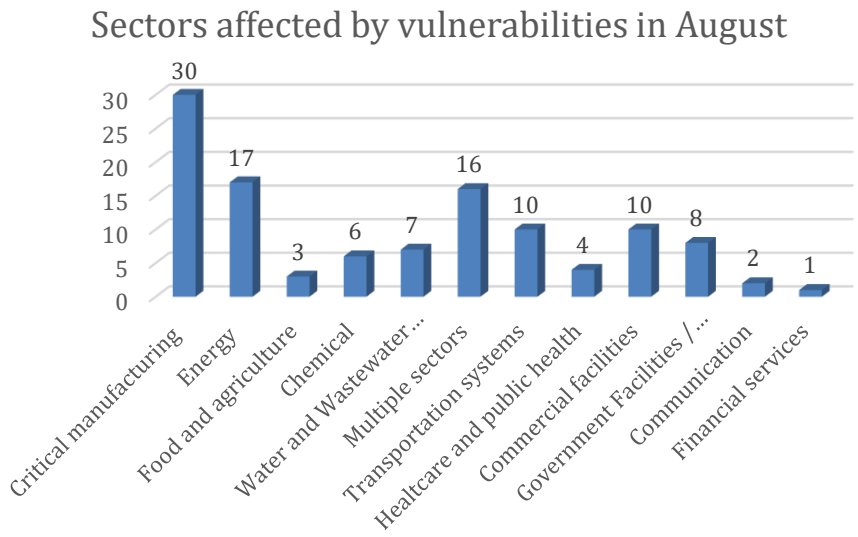
A variety of rapidly digitized critical infrastructure sectors in India — from finance to government systems and from manufacturing to healthcare — now are facing increased cyberattacks and cyber threats. ...

Source and more information:

https://www.darkreading.com/cyber-risk/india-s-critical-infrastructure-suffers-spike-in-cyberattacks

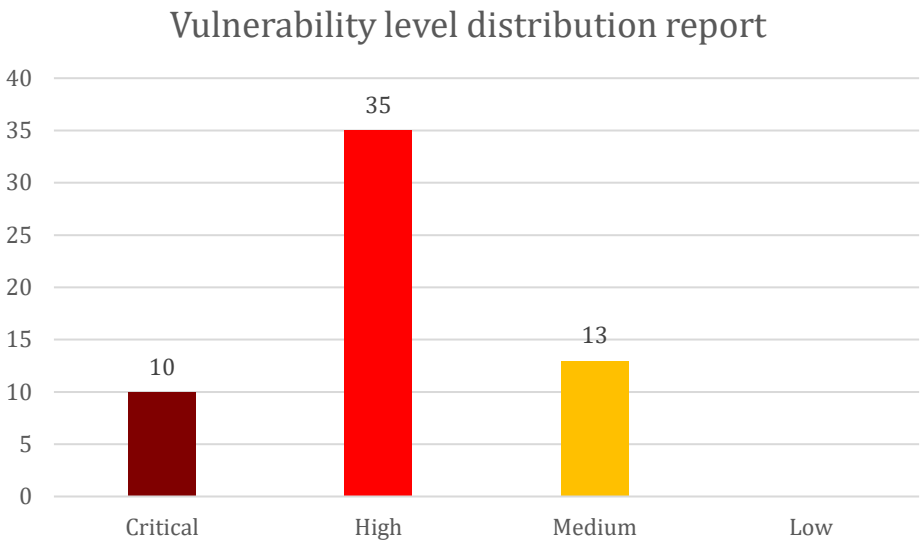
ICS vulnerabilities

In August 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 August:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	10
Out-of-bounds Read	CWE-125	6
Path Traversal	CWE-22	5
Allocation of Resources Without Limits or Throttling	CWE-770	5
Uncontrolled Resource Consumption	CWE-400	4
Incorrect Permission Assignment for Critical Resource	CWE-732	4



ICSA-24-242-01: **Rockwell Automation ThinManager ThinServer**

Critical level vulnerabilities: Improper Privilege Management, Incorrect Permission Assignment for Critical Resource, Improper Input Validation.

Rockwell Automation ThinManager ThinServer | CISA

ICSA-24-242-02: **Delta Electronics DTN Soft**

High level vulnerability: Deserialization of Untrusted Data.

Delta Electronics DTN Soft | CISA

ICSA-24-226-06: **Rockwell Automation FactoryTalk View Site Edition (Update A)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Rockwell Automation FactoryTalk View Site Edition (Update A) | CISA

SSA-999588: **Siemens User Management Component (UMC) Before V2.11.2 (Update 1.4.)**

High level vulnerabilities: Permissive Cross-domain Policy with Untrusted Domains, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Input Validation.

SSA-999588 (siemens.com)

SSA-981975: **Intel-CPUs (CVE-2022-40982) Impacting Siemens SIMATIC IPCs (Update 1.3.)**

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

SSA-981975 (siemens.com)

SSA-857368: **Siemens Omnivise T3000 (Update 1.1.)**

High level vulnerabilities: Files or Directories Accessible to External Parties, Cleartext Storage of Sensitive Information, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Input Validation.

SSA-857368 (siemens.com)

SSA-822518: **Palo Alto Networks Virtual NGFW Before V11.0.1 on Siemens RUGGEDCOM APE1808 Devices (Update 1.1.)**

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.

SSA-822518 (siemens.com)

SSA-813746: **Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families (Update 1.1.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-813746 (siemens.com)

SSA-771940: **Siemens Teamcenter Visualization and JT2Go (Update 1.1.)**

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

SSA-771940 (siemens.com)

SSA-750499: **Siemens SIPROTEC 5 Devices (Update 1.1.)**

High level vulnerability: Inadequate Encryption Strength.

SSA-750499 (siemens.com)

SSA-722010: **Siemens Teamcenter Visualization and JT2Go (Update 1.1.)**

High level vulnerability: Out-of-bounds Read.

SSA-722010 (siemens.com)

SSA-698820: **Siemens RUGGEDCOM APE1808 Devices (Update 1.1.)**

High level vulnerabilities: Stack-based Buffer Overflow, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incorrect Parsing of Numbers with Different Radices.

SSA-698820 (siemens.com)

SSA-686975: **Siemens Industrial Products using Intel CPUs (Update 1.5.)**

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

SSA-686975 (siemens.com)

SSA-640968: **Siemens TIA Project-Server formerly known as TIA Multiuser Server (Update 1.2.)**

Medium level vulnerability: Untrusted Search Path.

SSA-640968 (siemens.com)

SSA-625850: **Siemens Desigo CC Product Family and SENTRON powermanager (Update 1.1.)**

Critical level vulnerabilities: Buffer Over-read, Heap-based Buffer Overflow.

SSA-625850 (siemens.com)

SSA-407785: **Siemens Parasolid and Teamcenter Visualization (Update 1.3.)**

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 1.8.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-364175: **Palo Alto Networks Virtual NGFW on Siemens RUGGEDCOM APE1808 Devices (Update 1.1.)**

Critical level vulnerabilities: Truncation of Security-relevant Information, Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Improper Input Validation.

SSA-364175 (siemens.com)

SSA-180704: **Siemens SCALANCE M-800 Family Before V8.0 (Update 1.1.)**

Critical level vulnerabilities: Improper Validation of Specified Quantity in Input, Use of Hard-coded Cryptographic Key, Use of Weak Hash, 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, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

SSA-180704 (siemens.com)

SSA-116924: **Siemens TIA Portal (Update 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-116924 (siemens.com)

SSA-068047: **Siemens SCALANCE M-800 Family Before V7.2.2 (Update 1.1.)**

High level vulnerabilities: Acceptance of Extraneous Untrusted Data With Trusted Data, Direct Request ('Forced Browsing'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

SSA-068047 (siemens.com)

ICSA-24-235-01: **Rockwell Automation Emulate3D**

Medium level vulnerability: Externally Controlled Reference to a Resource in Another Sphere.

Rockwell Automation Emulate3D | CISA

ICSA-24-235-02: **Rockwell Automation 5015 – AENFTXT**

High level vulnerability: Improper Input Validation.

Rockwell Automation 5015 - AENFTXT | CISA

ICSA-24-235-03: **MOBOTIX P3 and Mx6 Cameras**

High level vulnerability: Improper Neutralization of Expression/Command Delimiters.

MOBOTIX P3 and Mx6 Cameras | CISA

ICSA-24-235-04: **Avtec Outpost 0810**

High level vulnerabilities: Storage of File with Sensitive Data Under Web Root, Use of Hard-coded Cryptographic Key.

Avtec Outpost 0810 | CISA

ICSA-20-282-02: **Mitsubishi Electric MELSEC iQ-R Series (Update D)**

High level vulnerability: Uncontrolled Resource Consumption.

Mitsubishi Electric MELSEC iQ-R Series (Update D) | CISA

ICSA-24-228-01: **Siemens SCALANCE M-800, RUGGEDCOM RM1224**

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Input Validation, Exposure of Data Element to Wrong Session, Insertion of Sensitive Information into Log File.

Siemens SCALANCE M-800, RUGGEDCOM RM1224 | CISA

ICSA-24-228-02: **Siemens INTRALOG WMS**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Heap-based Buffer Overflow.

Siemens INTRALOG WMS | CISA

ICSA-24-228-03: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: Out-of-bounds Read, NULL Pointer Dereference.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-228-04: **Siemens SINEC Traffic Analyzer**

High level vulnerabilities: Improper Privilege Management, Improper Restriction of Excessive Authentication Attempts, Improper Access Control, Use of Cache Containing Sensitive Information, Improperly Implemented Security Check for Standard.

Siemens SINEC Traffic Analyzer | CISA

ICSA-24-228-05: **Siemens LOGO! V8.3 BM Devices**

Medium level vulnerability: Plaintext Storage of a Password.

Siemens LOGO! V8.3 BM Devices | CISA

ICSA-24-228-06: **Siemens SINEC NMS**

Critical level vulnerabilities: Use After Free, Improper Input Validation, Deserialization of Untrusted Data, Improper Restriction of Operations within the Bounds of a Memory Buffer, Uncontrolled Resource Consumption, Out-of-bounds Read, Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'), Privilege Dropping / Lowering Errors, Allocation of Resources Without

Limits or Throttling, Execution with Unnecessary Privileges, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Incorrect Authorization.

Siemens SINEC NMS | CISA

ICSA-24-228-07: **Siemens Location Intelligence**

Medium level vulnerabilities: Inadequate Encryption Strength, Improper Restriction of Excessive Authentication Attempts, Weak Password Requirements.

Siemens Location Intelligence | CISA

ICSA-24-228-08: **Siemens COMOS**

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

Siemens COMOS | CISA

ICSA-24-228-09: **Siemens NX**

High level vulnerability: Out-of-bounds Read.

Siemens NX | CISA

ICSA-24-228-10: **AVEVA Historian Web Server**

High level vulnerability: SQL Injection.

AVEVA Historian Web Server | CISA

ICSA-24-228-11: **PTC Kepware ThingWorx Kepware Server**

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

PTC Kepware ThingWorx Kepware Server | CISA

ICSA-24-226-01: **AVEVA SuiteLink Server**

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

AVEVA SuiteLink Server | CISA

ICSA-24-226-02: **Rockwell Automation AADvance Standalone OPC-DA Server**

Critical level vulnerabilities: Improper Input Validation, Use of Externally Controlled Format String.

Rockwell Automation AADvance Standalone OPC-DA Server | CISA

ICSA-24-226-03: **Rockwell Automation GuardLogix/ControlLogix 5580 Controller**

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

Rockwell Automation GuardLogix/ControlLogix 5580 Controller | CISA

ICSA-24-226-04: **Rockwell Automation Pavilion8**

Medium level vulnerability: Missing Encryption of Sensitive Data.

Rockwell Automation Pavilion8 | CISA

ICSA-24-226-05: **Rockwell Automation DataMosaix Private Cloud**

High level vulnerability: Improper Authentication.

Rockwell Automation DataMosaix Private Cloud | CISA

ICSA-24-226-06: **Rockwell Automation FactoryTalk View Site Edition**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Rockwell Automation FactoryTalk View Site Edition | CISA

ICSA-24-226-07: **Rockwell Automation Micro850/870**

Medium level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation Micro850/870 | CISA

ICSA-24-226-08: **Ocean Data Systems Dream Report**

High level vulnerabilities: Path Traversal, Incorrect Permission Assignment for Critical Resource.

Ocean Data Systems Dream Report | CISA

ICSA-24-226-09: **Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix, Compact GuardLogix 5380**

High level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix, Compact GuardLogix 5380 | CISA

ICSA-24-226-10: **Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix, and Compact GuardLogix 5380**

High level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix, GuardLogix 5580, CompactLogix, and Compact GuardLogix 5380 | CISA

ICSA-24-221-01: **Dorsett Controls InfoScan**

Medium level vulnerability: Exposure of Sensitive Information To An Unauthorized Actor, Path Traversal.

Dorsett Controls InfoScan | CISA

ICSA-24-219-01: **Delta Electronics DIAScreen**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics DIAScreen | CISA

ICSA-24-214-01: **Johnson Controls exacqVision Client and exacqVision Server**

Critical level vulnerability: Inadequate Encryption Strength.

Johnson Controls exacqVision Client and exacqVision Server | CISA

ICSA-24-214-02: **Johnson Controls exacqVision Web Service**

High level vulnerability: Permissive Cross-domain Policy with Untrusted Domains.

Johnson Controls exacqVision Web Service | CISA

ICSA-24-214-03: **Johnson Controls exacqVision Web Service**

Medium level vulnerability: Cross-Site Request Forgery (CSRF).

Johnson Controls exacqVision Web Service | CISA

ICSA-24-214-04: **Johnson Controls exacqVision Web Service**

Medium level vulnerability: Cleartext Transmission of Sensitive Information.

Johnson Controls exacqVision Web Service | CISA

ICSA-24-214-05: **Johnson Controls exacqVision Server**

Medium level vulnerability: Improper Certificate Validation.

Johnson Controls exacqVision Server | CISA

ICSA-24-214-06: **Johnson Controls exacqVision Web Service**

Medium level vulnerability: Use of GET Request Method With Sensitive Query Strings.

Johnson Controls exacqVision Web Service | CISA

ICSA-24-214-07: **AVTECH IP Camera**

Critical level vulnerability: Command Injection.

AVTECH IP Camera | CISA

ICSA-24-214-08: **Vonets WiFi Bridges**

Critical level vulnerabilities: Use of Hard-coded Credentials, Improper Access Control, Path Traversal, Command Injection, Improper Check or Handling of Exceptional Conditions, Stack Based Buffer Overflow, Direct Request.

Vonets WiFi Bridges | CISA

ICSA-24-214-09: **Rockwell Automation Logix Controllers**

High level vulnerability: Unprotected Alternate Channel.

Rockwell Automation Logix Controllers | 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 August:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2018-0824 Microsoft COM for Windows Deserialization of Untrusted Data Vulnerability;
CVE-2024-36971 Android Kernel Remote Code Execution Vulnerability;
CVE-2024-32113 Apache OFBiz Path Traversal Vulnerability;
CVE-2024-38189 Microsoft Project Remote Code Execution Vulnerability;
CVE-2024-38178 Microsoft Windows Scripting Engine Memory Corruption Vulnerability;
CVE-2024-38213 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability;
CVE-2024-38193 Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability;
CVE-2024-38106 Microsoft Windows Kernel Privilege Escalation Vulnerability;
CVE-2024-38107 Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability;
CVE-2024-28986 SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability;
CVE-2024-23897 Jenkins Command Line Interface (CLI) Path Traversal Vulnerability;
CVE-2021-33044 Dahua IP Camera Authentication Bypass Vulnerability;
CVE-2021-33045 Dahua IP Camera Authentication Bypass Vulnerability;
CVE-2022-0185 Linux Kernel Heap-Based Buffer Overflow;
CVE-2021-31196 Microsoft Exchange Server Information Disclosure Vulnerability;
CVE-2024-39717 Versa Director Dangerous File Type Upload Vulnerability;
CVE-2024-7971 Google Chromium V8 Type Confusion Vulnerability;
CVE-2024-38856 Apache OFBiz Incorrect Authorization Vulnerability;
CVE-2024-7965 Google Chromium V8 Inappropriate Implementation 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 Six 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 Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog for Versa Networks Director | 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 Releases Secure by Demand Guidance

CISA and the Federal Bureau of Investigation (FBI) have released Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem to help organizations drive a secure technology ecosystem by ensuring their software manufacturers prioritize secure technology from the start.

Links and more information:

CISA Releases Secure by Demand Guidance | CISA

Royal Ransomware Actors Rebrand as "BlackSuit," FBI and CISA Release Update to Advisory

CISA—in partnership with the Federal Bureau of Investigation (FBI)—released an update to joint Cybersecurity Advisory #StopRansomware: Royal Ransomware, #StopRansomware: BlackSuit (Royal) Ransomware. The updated advisory provides network defenders with recent and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with BlackSuit and legacy Royal activity.

Links and more information:

Royal Ransomware Actors Rebrand as "BlackSuit," FBI and CISA Release Update to Advisory | CISA

Best Practices for Cisco Device Configuration

In recent incidents, CISA has seen malicious cyber actors acquire system configuration files by leveraging available protocols or software on devices, such as abusing the legacy Cisco Smart Install feature. CISA recommends organizations disable Smart Install and review NSA's Smart Install Protocol Misuse advisory and Network Infrastructure Security Guide for configuration guidance.

Links and more information:

Best Practices for Cisco Device Configuration | CISA

Microsoft Releases August 2024 Security Updates

Microsoft 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 August 2024 Security Updates | CISA

Ivanti Releases Security Updates for Avalanche, Neurons for ITSM, and Virtual Traffic Manager

Ivanti released security updates to address multiple vulnerabilities in Ivanti Avalanche, Neurons for ITSM, and Virtual Traffic Manager (vTM). A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system. Ivanti advises users to reduce their attack surface and follow industry best practices by adhering to Ivanti's network configuration guidance to restrict access to the management interface.

Links and more information:

Ivanti Releases Security Updates for Avalanche, Neurons for ITSM, and Virtual Traffic Manager | CISA

Adobe Releases Security Updates for Multiple Products

Adobe 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

ASD's ACSC, CISA, FBI, and NSA, with the support of International Partners Release Best Practices for Event Logging and Threat Detection

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), CISA, FBI, NSA, and international partners are releasing Best Practices for Event Logging and Threat Detection. This guide will assist organizations in defining a baseline for event logging to mitigate malicious cyber threats.

Links and more information:

ASD's ACSC, CISA, FBI, and NSA, with the support of International Partners Release Best Practices for Event Logging and Threat Detection | CISA

Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-39717

Versa Networks has released an advisory for a vulnerability (CVE-2024-39717) in Versa Director, a key component in managing SD-WAN networks, used by some Internet Service Providers (ISPs) and Managed Service Providers (MSPs). A cyber threat actor could exploit this vulnerability to take control of an affected system.

Links and more information:

Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-39717 | CISA

CISA and Partners Release Advisory on Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations

CISA—in partnership with the Federal Bureau of Investigation (FBI) and the Department of Defense Cyber Crime Center (DC3)—released Iran-based Cyber Actors Enabling Ransomware Attacks on U.S. Organizations.

Links and more information:

CISA and Partners Release Advisory on Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations | CISA

CISA and Partners Release Advisory on RansomHub Ransomware

CISA—in partnership with the Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), and Department of Health and Human Services (HHS)—released a joint Cybersecurity Advisory, #StopRansomware: RansomHub Ransomware.

Links and more information:

CISA and Partners Release Advisory on RansomHub Ransomware | CISA