2024 October, 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

Emphasizing Key Strategies and Best Practices for Managing Human Behavior to Enhance OT Security

The linked article highlights the crucial role human behavior plays in maintaining operational technology (OT) security. It presents best practices and strategies organizations can adopt to reduce the risks associated with human errors and behaviors, which can severely impact OT environments.

Key best practices include fostering a security culture that prioritizes awareness, training, and robust incident response procedures. Employees must be well-informed about security protocols and trained on how their actions affect the security of OT systems. Regular training, scenario-based exercises, and simulations are emphasized as effective tools for mitigating human-related risks.

A balanced approach is necessary to maintain both security and operational efficiency, especially in OT, where usability cannot be sacrificed for security. This requires the integration of security measures that complement usability, such as user-centered design principles and technologies that guide and influence human behavior, such as user behavior analytics and automated policy enforcement.

Moreover, effective governance through clear security policies, such as access controls and incident reporting procedures, is vital. Technology, in turn, should be used to support human behavior by offering real-time monitoring and feedback, further reinforcing a security-conscious culture.

Ultimately, the article underscores the importance of managing human behavior, not only through technological solutions but also by building a collaborative, security-focused organizational mindset. This approach ensures a significant improvement in OT security, safeguarding critical infrastructure against both intentional and unintentional security breaches.

By combining continuous training, technological aids, and a security-first culture, organizations can significantly reduce human-induced vulnerabilities in OT environments.

Source, links (where you can download the Masterplan) and more information available on the following link:

https://industrialcyber.co/features/emphasizing-key-strategies-and-best-practices-for-managing-human-behavior-to-enhance-ot-security/

ICS trainings, education

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

!NEW! in this ICS security feed:

- OT Railway Cybersecurity (OTCS)

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

ICS conferences

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

OT, ICS and SCADA Automation

OT, ICS and SCADA Automation celebrates 22 years of being the Asia Pacific region's best and largest Operational Technology and SCADA event. Formerly titled the National SCADA Conference the case studies and lessons learned from real implementations, not theory, are the key drivers for why Australia and New Zealand lead the globe. The conference and associated networking functions bring the industry together to network, learn, share stories and experiences. This year's programme will facilitate insightful debates on the most critical strategic, technical and business issues, for successful Operational Technology & SCADA systems. It will equip you and your team with up-to-date practical advice to make informed and profitable decisions.

Australia, Brisbane; 12th – 13th November 2024

More details can be found on the following website:

https://scada-conference.com/

19th Annual API Cybersecurity Conference for the Oil and Natural Gas Industry

The API Cybersecurity Conference has been an annual event since 2006. For 18 years it has been the only cybersecurity conference dedicated to the oil and natural gas industry and has a loyal and dedicated attendee base. It is also volunteer-driven, both at the planning committee and speaker level. We consistently produce a compelling conference program, with a focus on safety, best practices, and innovation. In addition, the conference provides an opportunity for attendees to earn CPEs (Continuing Professional Education), maintaining their certifications and required hours. Finally, the conference provides the opportunity for networking and idea exchange, with our dedicated sponsors and exhibitors sharing their latest products and services.

USA, The Woodlands, Texas; 12th – 13th November 2024

More details can be found on the following website:

https://events.api.org/19th-annual-api-cybersecurity-conference-for-the-oil-and-natural-gas-industry/

Industrial Security Conference Copenhagen

Networking in the field of industrial security is key to staying ahead of threats and protecting vital infrastructure. ISC-CPH 12-13-14 November is one of Europe's fastest growing networking event on industrial security that helps you strengthen your defenses, share knowledge, build new alliances and gain new insights.

With a program, crafted by a top-tier advisory board in collaboration with ISACA and ICC, we will unpack the latest strategies, technologies, and ensure you new insights on topics such as contingency plans, NIS2, resilience, Risk assessment, priority strategies, and supply chain security.

Denmark, Copenhagen; 12th – 14th November 2024

More details can be found on the following website:

https://insightevents.dk/isc-cph/

ICS incidents

American Water shuts down online services after cyberattack

American Water, the largest publicly traded water and wastewater utility company in the U.S., was the target of a cyberattack that forced the company to shut down certain systems. The incident led to disruptions in its customer services, particularly the MyWater online portal and billing services. In response, American Water immediately hired third-party cybersecurity experts to assess and contain the breach. The company also reported the event to law enforcement, who are working jointly with the company in an ongoing investigation.

In an official filing with the U.S. Securities and Exchange Commission (SEC), American Water outlined the steps taken to safeguard its systems and data, including temporarily disconnecting certain systems to prevent further damage. Despite the disruption, a company spokesperson, Ruben Rodriguez, assured customers that there would be no late charges while systems were down. Rodriguez also stated that the water and wastewater operations had not been impacted by the attack.

This incident comes in the wake of other recent cyberattacks targeting U.S. water utilities, including a breach at the water treatment facility in Arkansas City, Kansas, which had to switch to manual operations due to a cyberattack.

The increasing frequency of such attacks has raised concerns across the water sector. The Water Information Sharing and Analysis Center (WaterISAC), a nonprofit organization focused on protecting water utilities from cyber threats, issued a warning of Russian-linked cyberattacks targeting the sector. Additionally, the U.S. Environmental Protection Agency (EPA) recently issued guidance to help water and wastewater systems enhance their cybersecurity practices.

The attack on American Water is part of a larger trend of cyber threats facing critical infrastructure, with recent examples including Chinese-backed Volt Typhoon hackers and Iranian threat actors breaching U.S. water facilities in 2023. These events underscore the vulnerability of essential services to cyberattacks and highlight the need for strengthened security measures in the water sector.

The source is available on the following link:

https://cybernews.com/news/duvel-moortgat-ransomware-attack/

Book recommendation

Cyber Security: Critical Infrastructure Protection

This book focus on critical infrastructure protection. The chapters present detailed analysis of the issues and challenges in cyberspace and provide novel solutions in various aspects. The first part of the book focus on digital society, addressing critical infrastructure and different forms of the digitalization, strategic focus on cyber security, legal aspects on cyber security, citizen in digital society, and cyber security training.

The second part focus on the critical infrastructure protection in different areas of the critical infrastructure. The chapters cover the cybersecurity situation awareness, aviation and air traffic control, cyber security in smart societies and cities, cyber security in smart buildings, maritime cyber security, cyber security in energy systems, and cyber security in healthcare.

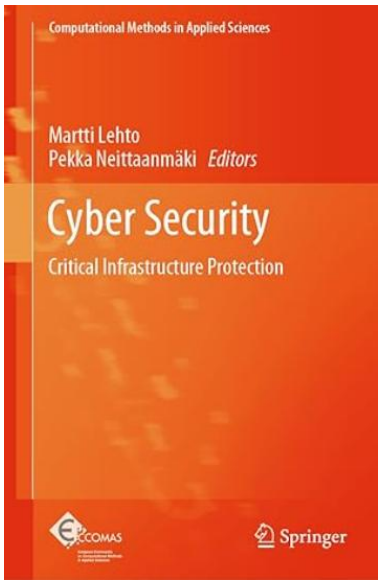
The third part presents the impact of new technologies upon cyber capability building as well as new challenges brought about by new technologies. These new technologies are among others are quantum technology, firmware and wireless technologies, malware analysis, virtualization.

Author/Editor: Martti Lehto, Pekka Neittaanmäki (Editors)

Year of issue: 2022

The book is available at the following link:

https://link.springer.com/book/10.1007/978-3-030-91293-2



ICS security news selection

Can You Identify Your Critical Business Functions — and Their Technology Dependencies?

Identifying your organization's critical business functions is foundational to all kinds of strategic planning initiatives. Every organization has a definitive list that they review at least annually, right? Not so much, it turns out.

Most lists of critical business functions are too high-level to be actionable. In a world where billions of assets are connected to the internet and each other, the definition of critical business functions must include dependencies that could contribute to a larger failure if they were damaged or disrupted. This is especially true of operational technology (OT) and Internet of Things (IoT) assets that control physical and digital processes, which often are omitted entirely from such lists. …

Source and more information:

https://industrialcyber.co/expert/can-you-identify-your-critical-business-functions-and-their-technology-dependencies/

NSA Releases 6 Principles of OT Cybersecurity

The National Security Agency (NSA) joined cybersecurity agencies from Australia, Canada, Germany, Japan, the Netherlands, New Zealand, South Korea, and the United Kingdom to publish a guide outlining six principles that can be used to guide the creation and maintenance of a safe, security critical infrastructure operational technology (OT) environment. "Principles of Operational Technology Cyber Security" offers security practitioners ways to bolster the security of critical infrastructure, including water, energy, and transportation systems. …

Source and more information:

https://www.darkreading.com/ics-ot-security/nsa-releases-6-principles-ot-cybersecurity

Ransomware Hits Critical Infrastructure Hard, Costs Adding Up

The financial impact of a cyberattack targeting a cyber-physical system (CPS) can reach up to $1 million, as affected organizations struggle with revenue loss, recovery costs, and employee overtime.

According to a new Claroty survey of 1,100 security professionals involved in OT, IoT, BMS, and IoMT (connected medical devices), about 45% of organizations suffered losses of $500,000 or more over the past year, while 27% disclosed losses of $1 million or more. …

Source and more information:

https://www.securityweek.com/ransomware-hits-critical-infrastructure-hard-costs-adding-up/

Growing need to balance benefits, risks of integrating AI in OT cybersecurity in evolving threat landscape

As OT (operational technology) environments are increasingly bombarded with sophisticated cyber threats and attacks, it emerges critically promising to integrate AI into OT cybersecurity, offering a much-needed upgrade. AI (artificial intelligence) may analyze huge amounts of data in real-time, thereby significantly helping to enhance the threat detection and response capabilities against an evolving adversary. However, there also lies a dual-edged sword in introducing AI in OT cybersecurity, requiring a rather careful balancing of benefits against the inherent risks of such emerging technology across critical OT environments. …

Source and more information:

https://industrialcyber.co/ai/growing-need-to-balance-benefits-risks-of-integrating-ai-in-ot-cybersecurity-in-evolving-threat-landscape/

Organizations Faster at Detecting OT Incidents, but Response Still Lacking: Report

Organizations have been getting faster at detecting incidents in industrial control system (ICS) and other operational technology (OT) environments, but incident response is still lacking, according to a new report from the SANS Institute.

SANS's 2024 State of ICS/OT Cybersecurity report, which is based on a survey of more than 530 professionals in critical infrastructure sectors, shows that roughly 60% of

respondents can detect a compromise in less than 24 hours, which is a significant improvement compared to five years ago when the same number of respondents said their compromise-to-detection time had been 2-7 days. …

Source and more information:

https://www.securityweek.com/organizations-faster-at-detecting-ot-incidents-but-response-still-lacking-report/

Rise of women in ICS: Transforming industrial landscape with fresh perspectives

With the rapid evolution of the industrial cybersecurity sector, women are increasingly penetrating the space that was for a long time controlled and influenced by the male population. Approximately 12 percent of the ICS (industrial control systems) security community is made up of women. Entering and succeeding in this male-dominated field can be challenging due to intentional and unintentional discrimination. However, women are contributing fresh perspectives and innovative solutions, transforming the industrial landscape. Also, there exists across the industry a commitment to empowering women in ICS by creating leadership and innovation opportunities. …

Source and more information:

https://industrialcyber.co/features/rise-of-women-in-ics-transforming-industrial-landscape-with-fresh-perspectives/

OT PCAP Analyzer: Free PCAP analysis tool

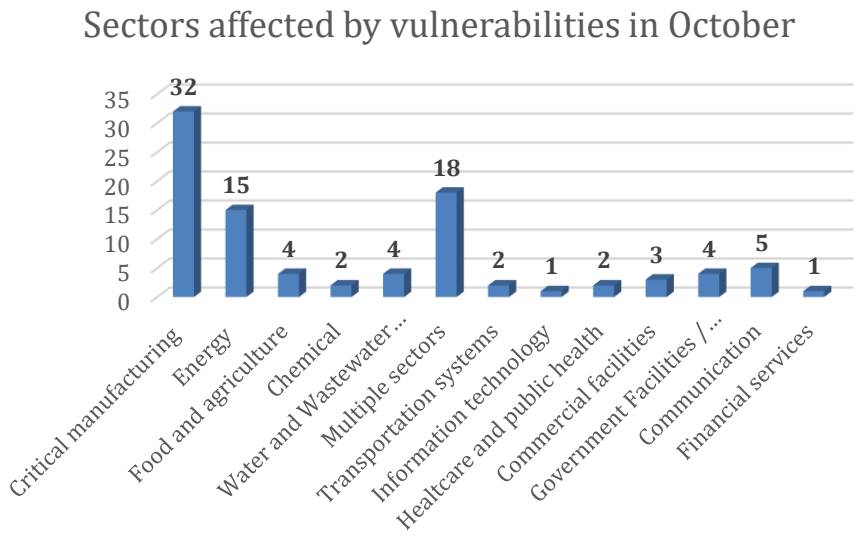
EmberOT's OT PCAP Analyzer, developed for the industrial security community, is a free tool providing a high-level overview of the devices and protocols in packet capture files. "The OT PCAP Analyzer was designed specifically with critical OT environments in mind. We've created a novel set of engines to gather and analyze network traffic at speed with unparalleled accuracy. This allows the free PCAP Analyzer to quickly identify OT devices, protocols, and how those elements interact. We stream this data in real-time so the user can begin reviewing results while a .pcap or .pcapng is being processed," Jori VanAntwerp, CEO of EmberOT, told Help Net Security. …

Source and more information:

https://www.helpnetsecurity.com/2024/10/29/ot-pcap-analyzer-free-pcap-analysis-tool/

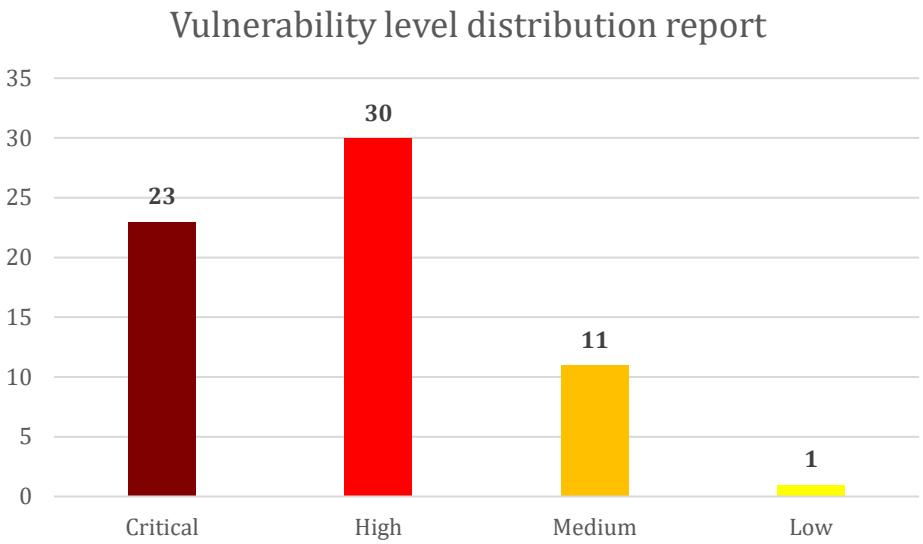
ICS vulnerabilities

In October 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 October:

Vulnerability	CWE number	Items
Missing Authentication for Critical Function	CWE-306	9
Improper Input Validation	CWE-20	5
Out-of-bounds Read	CWE-125	5
Cross-site Scripting	CWE-79	5
Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE-119	5



ICSA-24-305-01: **Rockwell Automation FactoryTalk ThinManager**

Critical level vulnerabilities: Missing Authentication For Critical Function, Out-of-Bounds Read.

Rockwell Automation FactoryTalk ThinManager | CISA

ICSA-24-030-02: **Mitsubishi Electric FA Engineering Software Products (Update A)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Unsafe Reflection.

Mitsubishi Electric FA Engineering Software Products (Update A) | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update A)**

Low level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write, Improper Privilege Management.

Mitsubishi Electric Multiple FA Engineering Software Products (Update A) | CISA

ICSA-23-157-02: **Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series (Update B)**

High level vulnerabilities: Weak Password Requirements, Use of Hard-coded Credentials, Missing Password Field Masking, Unrestricted Upload of File with Dangerous Type.

Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series (Update B) | CISA

ICSA-24-303-01: **Siemens InterMesh Subscriber Devices**

Critical level vulnerabilities: OS Command Injection, Missing Authentication for Critical Function, Execution with Unnecessary Privileges, Incorrect Privilege Assignment.

Siemens InterMesh Subscriber Devices | CISA

ICSA-24-303-02: **Solar-Log Base 15**

Medium level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Solar-Log Base 15 | CISA

ICSA-24-303-03: **Delta Electronics InfraSuite Device Master**

Critical level vulnerability: Deserialization of Untrusted Data.

Delta Electronics InfraSuite Device Master | CISA

ICSA-24-298-01: **VIMESA VHF/FM Transmitter Blue Plus**

Medium level vulnerability: Improper Access Control.

VIMESA VHF/FM Transmitter Blue Plus | CISA

ICSA-24-298-02: **iniNet Solutions SpiderControl SCADA PC HMI Editor**

High level vulnerability: Path Traversal.

iniNet Solutions SpiderControl SCADA PC HMI Editor | CISA

ICSA-24-298-03: **Deep Sea Electronics DSE855**

High level vulnerability: Missing Authentication for Critical Function.

Deep Sea Electronics DSE855 | CISA

ICSA-24-268-06: **OMNTEC Proteus Tank Monitoring (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

OMNTEC Proteus Tank Monitoring (Update A) | CISA

ICSA-24-296-01: **ICONICS and Mitsubishi Electric Products**

High level vulnerability: Incorrect Default Permissions.

ICONICS and Mitsubishi Electric Products | CISA

ICSA-24-291-01: **Elvaco M-Bus Metering Gateway CMe3100**

Critical level vulnerabilities: Missing Authentication for Critical Function, Unrestricted Upload of File with Dangerous Type, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Insufficiently Protected Credentials.

Elvaco M-Bus Metering Gateway CMe3100 | CISA

ICSA-24-291-02: **LCDS LAquis SCADA**

High level vulnerability: Cross-site Scripting.

LCDS LAquis SCADA | CISA

ICSA-24-291-03: **Mitsubishi Electric CNC Series**

Medium level vulnerability: Improper Validation of Specified Quantity in Input.

Mitsubishi Electric CNC Series | CISA

ICSA-24-291-04: **HMS Networks EWON FLEXY 202**

High level vulnerability: Insufficiently Protected Credentials.

HMS Networks EWON FLEXY 202 | CISA

ICSA-24-291-05: **Kieback&Peter DDC4000 Series**

Critical level vulnerabilities: Path Traversal, Insufficiently Protected Credentials, Use of Weak Credentials.

Kieback&Peter DDC4000 Series | CISA

ICSA-24-270-04: **goTenna Pro X and Pro X2 (Update A)**

High level vulnerabilities: Weak Password Requirements, Insecure Storage of Sensitive Information, Missing Support for Integrity Check, Cleartext Transmission of Sensitive Information, Improper Restriction of Communication Channel to Intended Endpoints, Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Weak Authentication, Insertion of Sensitive Information Into Sent Data, Observable Response Discrepancy, Missing Authentication for Critical Function.

goTenna Pro X and Pro X2 (Update A) | CISA

ICSA-24-270-05: **goTenna Pro ATAK Plugin (Update A)**

High level vulnerabilities: Weak Password Requirements, Insecure Storage of Sensitive Information, Missing Support for Integrity Check, Cleartext Transmission of Sensitive Information, Use of Cryptographically Weak Pseudo-Random Number

Generator (PRNG), Weak Authentication, Insertion of Sensitive Information Into Sent Data, Observable Response Discrepancy, Insertion of Sensitive Information Into Sent Data.

goTenna Pro ATAK Plugin (Update A) | CISA

ICSA-24-289-01: **Siemens Siveillance Video Camera**

High level vulnerability: Classic Buffer Overflow.

Siemens Siveillance Video Camera | CISA

ICSA-24-289-02: **Schneider Electric Data Center Expert**

High level vulnerabilities: Improper Verification of Cryptographic Signature, Missing Authentication for Critical Function.

Schneider Electric Data Center Expert | CISA

SSA-097435: **Siemens Mendix Runtime (Update 1.3.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435 (siemens.com)

SSA-999588: **Siemens User Management Component (UMC) Before V2.11.2 (Update 1.6.)**

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-962515: **Siemens Industrial Products (Update 1.3.)**

High level vulnerability: Out-of-bounds Read.

SSA-962515 (siemens.com)

SSA-955858: **Siemens LOGO! 8 BM Devices (Update 1.3.)**

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-921449: **Siemens LOGO! V8.3 BM Devices (Update 1.2.)**

Medium level vulnerability: Plaintext Storage of a Password.

SSA-921449 (siemens.com)

SSA-844582: **Siemens LOGO! V8.3 BM Devices Results in Broken LOGO! V8.3 Product CA (Update 1.2.)**

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

SSA-844582 (siemens.com)

SSA-783481: **Siemens LOGO! 8 BM (Update 1.3.)**

Medium level vulnerability: Improper Handling of Exceptional Conditions.

SSA-783481 (siemens.com)

SSA-711309: **OPC UA Implementations of Siemens SIMATIC Products (Update 2.1.)** **High** level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-698820: **Fortigate NGFW Before V7.4.4 on Siemens RUGGEDCOM APE1808 Devices (Update 1.3.)**

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, Improper Access Control.

SSA-698820 (siemens.com)

SSA-629254: **Siemens SIMATIC SCADA and PCS 7 systems (Update 1.1.)**

Critical level vulnerability: Execution with Unnecessary Privileges.

SSA-629254 (siemens.com)

SSA-620288: **Capital Embedded AR Classic (Update 1.2.)**

High level vulnerabilities: Access of Resource Using Incompatible Type ('Type Confusion'), Improper Validation of Specified Quantity in Input, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Integer Underflow (Wrap or Wraparound), Improper Handling of Inconsistent Structural Elements.

SSA-620288 (siemens.com)

SSA-455250: **Palo Alto Networks Virtual NGFW on Siemens RUGGEDCOM APE1808 Devices Before V11.1.2-h3 (Update 1.4.)**

Critical level vulnerabilities: Multiple.

SSA-455250 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 1.9.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-366067: **Fortigate NGFW Before V7.4.1 on Siemens RUGGEDCOM APE1808 Devices (Update 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-366067 (siemens.com)

SSA-364175: **Palo Alto Networks Virtual NGFW on Siemens RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update 1.2.)**

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-321292: **Siemens Industrial Products (Update 1.6.)**

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

SSA-321292 (siemens.com)

SSA-148641: **Mendix Runtime (Update 1.3.)**

Medium level vulnerability: Improper Access Control.

SSA-148641 (siemens.com)

SSA-039007: **Siemens User Management Component (UMC) (Update 1.1.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-039007 (siemens.com)

ICSA-24-284-01: **Siemens SIMATIC S7-1500 and S7-1200 CPUs**

Medium level vulnerability: Open Redirect.

Siemens SIMATIC S7-1500 and S7-1200 CPUs | CISA

ICSA-24-284-02: **Siemens Simcenter Nastran**

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

Siemens Simcenter Nastran | CISA

ICSA-24-284-03: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: Stack-based Buffer Overflow, NULL Pointer Dereference.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-284-04: **Siemens SENTRON PAC3200 Devices**

Critical level vulnerability: Improper Authentication.

Siemens SENTRON PAC3200 Devices | CISA

ICSA-24-284-05: **Siemens Questa and ModelSim**

Medium level vulnerability: Uncontrolled Search Path Element.

Siemens Questa and ModelSim | CISA

ICSA-24-284-06: **Siemens SINEC Security Monitor**

Critical level vulnerabilities: Argument Injection, Command Injection, Path Traversal, Permissive List of Allowed Inputs.

Siemens SINEC Security Monitor | CISA

ICSA-24-284-07: **Siemens JT2Go**

High level vulnerability: Stack-based Buffer Overflow.

Siemens JT2Go | CISA

ICSA-24-284-08: **Siemens HiMed Cockpit**

Critical level vulnerability: Improper Protection of Alternate Path.

Siemens HiMed Cockpit | CISA

ICSA-24-284-09: **Siemens PSS SINCAL**

Critical level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens PSS SINCAL | CISA

ICSA-24-284-10: **Siemens SIMATIC S7-1500 CPUs**

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

Siemens SIMATIC S7-1500 CPUs | CISA

ICSA-24-284-11: **Siemens RUGGEDCOM APE1808**

Medium level vulnerability: Incorrect Authorization.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-284-12: **Siemens Sentron Powercenter 1000**

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

Siemens Sentron Powercenter 1000 | CISA

ICSA-24-284-13: **Siemens Tecnomatix Plant Simulation**

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.

Siemens Tecnomatix Plant Simulation | CISA

ICSA-24-284-14: **Schneider Electric Zelio Soft 2**

High level vulnerabilities: Use After Free, Improper Input Validation.

Schneider Electric Zelio Soft 2 | CISA

ICSA-24-284-15: **Rockwell Automation DataMosaix Private Cloud**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Missing Authorization, Incorrect Authorization.

Rockwell Automation DataMosaix Private Cloud | CISA

ICSA-24-284-16: **Rockwell Automation DataMosaix Private Cloud**

Critical level vulnerabilities: Inadequate Encryption Strength, Out-of-bounds Write, Improper Check for Dropped Privileges, Reliance on Insufficiently Trustworthy Component, NULL Pointer Dereference.

Rockwell Automation DataMosaix Private Cloud | CISA

ICSA-24-284-17: **Rockwell Automation Verve Asset Manager**

High level vulnerability: Placement of User into Incorrect Group.

Rockwell Automation Verve Asset Manager | CISA

ICSA-24-284-18: **Rockwell Automation Logix Controllers**

High level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation Logix Controllers | CISA

ICSA-24-284-19: **Rockwell Automation PowerFlex 6000T**

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

Rockwell Automation PowerFlex 6000T | CISA

ICSA-24-284-20: **Rockwell Automation ControlLogix**

High level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix | CISA

ICSA-24-284-21: **Delta Electronics CNCSoft-G2**

High level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Write, Heap-Based Buffer Overflow, Out-of-bounds Read, Use of Uninitialized Variable.

Delta Electronics CNCSoft-G2 | CISA

ICSA-24-277-01: **TEM Opera Plus FM Family Transmitter**

Critical level vulnerabilities: Missing Authentication for Critical Function, Cross-Site Request Forgery (CSRF).

TEM Opera Plus FM Family Transmitter | CISA

ICSA-24-277-02: **Subnet Solutions Inc. PowerSYSTEM Center**

High level vulnerabilities: Server-Side Request Forgery (SSRF), Inefficient Regular Expression Complexity, Cross-Site Request Forgery (CSRF).

Subnet Solutions Inc. PowerSYSTEM Center | CISA

ICSA-24-277-03: **Delta Electronics DIAEnergie**

Critical level vulnerability: SQL Injection.

Delta Electronics DIAEnergie | CISA

ICSA-24-275-01: **Optigo Networks ONS-S8 Spectra Aggregation Switch**

Critical level vulnerabilities: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion'), Weak Authentication.

Optigo Networks ONS-S8 Spectra Aggregation Switch | CISA

ICSA-24-275-02: **Mitsubishi Electric MELSEC iQ-F FX5-OPC**

High level vulnerability: NULL Pointer Dereference.

Mitsubishi Electric MELSEC iQ-F FX5-OPC | 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 October:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-29824 Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability;
CVE-2024-45519 Synacor Zimbra Collaboration Command Execution Vulnerability;
CVE-2024-43047 Qualcomm Multiple Chipsets Use-After-Free Vulnerability;
CVE-2024-43572 Microsoft Windows Management Console Remote Code Execution Vulnerability;
CVE-2024-43573 Microsoft Windows MSHTML Platform Spoofing Vulnerability;
CVE-2024-23113 Fortinet Multiple Products Format String Vulnerability;
CVE-2024-9379 Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability;
CVE-2024-9380 Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability;
CVE-2024-30088 Microsoft Windows Kernel TOCTOU Race Condition Vulnerability;
CVE-2024-9680 Mozilla Firefox Use-After-Free Vulnerability;
CVE-2024-28987 SolarWinds Web Help Desk Hardcoded Credential Vulnerability;
CVE-2024-40711 Veeam Backup and Replication Deserialization Vulnerability;
CVE-2024-9537 ScienceLogic SL1 Unspecified Vulnerability;
CVE-2024-38094 Microsoft SharePoint Deserialization Vulnerability;
CVE-2024-47575 Fortinet FortiManager Missing Authentication Vulnerability;
CVE-2024-20481 Cisco ASA and FTD Denial-of-Service Vulnerability;
CVE-2024-37383 RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
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 One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

ASD's ACSC, CISA, FBI, NSA, and International Partners Release Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organizations
Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)—in partnership with CISA, U.S. government and international partners—released the guide Principles of Operational Technology Cybersecurity. This guidance provides critical information on how to create and maintain a safe, secure operational technology (OT) environment.

Links and more information:
ASD's ACSC, CISA, FBI, NSA, and International Partners Release Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organizations | CISA

CISA and FBI Release Fact Sheet on Protecting Against Iranian Targeting of Accounts Associated with National Political Organizations

CISA and the Federal Bureau of Investigation (FBI) released joint fact sheet, How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations. This fact sheet provides information about threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) targeting and compromising accounts of Americans to stoke discord and undermine confidence in U.S. democratic institutions.

Links and more information:
CISA and FBI Release Fact Sheet on Protecting Against Iranian Targeting of Accounts Associated with National Political Organizations | CISA

Avoid Scams After Disaster Strikes

As hurricanes and other natural disasters occur, CISA urges individuals to remain on alert for potential malicious cyber activity. Fraudulent emails and social media messages—often containing malicious links or attachments—are common after major natural disasters. Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events. Before responding, ensure hurricane-related guidance is from trusted sources, such as local officials and disaster response organizations, including Federal Emergency Management Agency (FEMA) and DHS's Ready.gov.

Links and more information:
Avoid Scams After Disaster Strikes | CISA

Microsoft Releases October 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 October 2024 Security Updates | 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

Best Practices to Configure BIG-IP LTM Systems to Encrypt HTTP Persistence Cookies

CISA has observed cyber threat actors leveraging unencrypted persistent cookies managed by the F5 BIG-IP Local Traffic Manager (LTM) module to enumerate other non-internet facing devices on the network. F5 BIG-IP is a suite of hardware and software solutions designed to manage and secure network traffic. A malicious cyber actor could leverage the information gathered from unencrypted persistence cookies to infer or identify additional network resources and potentially exploit vulnerabilities found in other devices present on the network.

Links and more information:

Best Practices to Configure BIG-IP LTM Systems to Encrypt HTTP Persistence Cookies | CISA

Guidance: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)

CISA published the Framing Software Component Transparency, created by the Software Bill of Materials (SBOM) Tooling & Implementation Working Group, one of the five SBOM community-driven workstreams facilitated by CISA. CISA's community-driven working groups publish documents and reports to advance and refine SBOM and ultimately promote adoption. This resource serves as the detailed foundation of SBOM, defining SBOM concepts and related terms and offering an updated baseline of how software components are to be represented. This document serves as a guide on the processes around SBOM creation.

Links and more information:

Guidance: Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM) | CISA

CISA, FBI, NSA, and International Partners Release Advisory on Iranian Cyber Actors Targeting Critical Infrastructure Organizations Using Brute Force

CISA—with the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners—released joint Cybersecurity Advisory Iranian Cyber Actors Brute Force and Credential Access Activity Compromises Critical Infrastructure. This advisory provides known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by Iranian actors to impact organizations across multiple critical infrastructure sectors.

Links and more information:

CISA, FBI, NSA, and International Partners Release Advisory on Iranian Cyber Actors Targeting Critical Infrastructure Organizations Using Brute Force | CISA

CISA and FBI Release Joint Guidance on Product Security Bad Practices for Public Comment

Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released joint guidance on Product Security Bad Practices, a part of

CISA's Secure by Design initiative. This joint guidance supplies an overview of exceptionally risky product security bad practices for software manufacturers who produce software in support of critical infrastructure or national critical functions.
Links and more information:
CISA and FBI Release Joint Guidance on Product Security Bad Practices for Public Comment | CISA

Oracle Releases Quarterly Critical Patch Update Advisory for October 2024
Oracle released its quarterly Critical Patch Update Advisory for October 2024 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:
Oracle Releases Quarterly Critical Patch Update Advisory for October 2024 | CISA

CISA, US, and International Partners Release Joint Guidance to Assist Software Manufacturers with Safe Software Deployment Processes
CISA—along with U.S. and international partners—released joint guidance, Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers. This guide aids software manufacturers in establishing secure software deployment processes to help ensure software is reliable and safe for customers. Additionally, it offers guidance on how to deploy in an efficient manner as part of the software development lifecycle (SDLC).
Links and more information:
CISA, US, and International Partners Release Joint Guidance to Assist Software Manufacturers with Safe Software Deployment Processes | CISA

Cisco Releases Security Bundle for Cisco ASA, FMC, and FTD Software
Cisco released its October 2024 Semiannual Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication to address vulnerabilities in Cisco ASA, FMC, and FTD. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Cisco Releases Security Bundle for Cisco ASA, FMC, and FTD Software | 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

JCDC's Industry-Government Collaboration Speeds Mitigation of CrowdStrike IT Outage

CISA, through the Joint Cyber Defense Collaborative (JCDC), enabled swift, coordinated response and information sharing in the wake of a significant IT outage caused by a CrowdStrike software update. This outage, which impacted government, critical infrastructure, and industry across the globe, led to disruptions in essential services, including air travel, healthcare, and financial operations.

Links and more information:

JCDC's Industry-Government Collaboration Speeds Mitigation of CrowdStrike IT Outage | CISA

Fortinet Updates Guidance and Indicators of Compromise following FortiManager Vulnerability Exploitation

Fortinet has updated their security advisory addressing a critical FortiManager vulnerability (CVE-2024-47575) to include additional workarounds and indicators of compromise (IOCs). A remote, unauthenticated cyber threat actor could exploit this vulnerability to gain access to sensitive files or take control of an affected system. At this time, all patches have been released.

Links and more information:

Fortinet Updates Guidance and Indicators of Compromise following FortiManager Vulnerability Exploitation | CISA

Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments

CISA has received multiple reports of a large-scale spear-phishing campaign targeting organizations in several sectors, including government and information technology (IT). The foreign threat actor, often posing as a trusted entity, is sending spear-phishing emails containing malicious remote desktop protocol (RDP) files to targeted organizations to connect to and access files stored on the target's network. Once access has been gained, the threat actor may pursue additional activity, such as deploying malicious code to achieve persistent access to the target's network.

Links and more information:

Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments | CISA