2024 November, 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

Introduction to ICS/OT Systems and their Role in Critical Infrastructure

On the ISACA website, there is a blog post from last year that attempts to provide a comprehensive approach to ICS/OT security. In summary, the blog post covers the following:

Industrial Control Systems (ICS) and Operational Technology (OT) are crucial for managing critical infrastructure in sectors like manufacturing, energy, water, transportation, and healthcare. These systems combine hardware and software to control automated processes essential to societal and economic stability, making them vital targets for cybersecurity. Given the potential for significant impact, ICS/OT security has become a primary focus area for cybersecurity professionals.

Characteristics and Importance of ICS/OT Systems ICS/OT systems manage physical processes, such as power grids, water treatment facilities, and hospital equipment, and have specific requirements, like high reliability and the ability to operate in challenging environments. These attributes make it difficult to apply traditional IT security protocols, as ICS/OT systems prioritize uptime and performance over frequent updates and access restrictions. However, disruptions can lead to severe consequences, including environmental hazards, operational shutdowns, or even loss of life.

Primary Risks to ICS/OT Systems These systems are exposed to a range of cyber threats, including malware, phishing, and denial-of-service attacks. As cyberattacks become increasingly sophisticated, ICS/OT systems are more vulnerable—especially those connected to the internet. For instance, in 2015, Ukraine's power grid was attacked, causing a widespread blackout that impacted over 230,000 people. The attackers exploited ICS/OT system vulnerabilities to disrupt power, highlighting the importance of securing critical infrastructure.

Best Practices for Securing ICS/OT Systems Effective ICS/OT security begins with identifying system-specific risks through regular assessments. Key measures include network segmentation, which isolates ICS/OT networks to reduce vulnerability exposure, and strict access controls that limit system access to essential personnel. Monitoring, logging, and incident response planning enable timely detection and mitigation of potential breaches. Employee training is also essential, as awareness of social engineering tactics can reduce the risk of unauthorized access.

Organizations should employ specialized security tools tailored to ICS/OT environments, such as firewalls and intrusion detection systems designed for industrial

applications. These tools help detect and respond to unique threats within ICS/OT systems.

Ensuring Long-term Security Securing ICS/OT systems is critical for maintaining stable, safe infrastructure. By understanding system-specific characteristics and employing comprehensive risk assessments and controls, organizations can protect these essential assets from evolving cyber threats. Implementing best practices ensures that ICS/OT systems remain secure, resilient, and reliable, safeguarding vital infrastructure for society.

It is worth considering the information provided and extracting the key points as they apply to our own organization.

Source and more information available on the following link:

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/introduction-to-ics-ot-systems-and-their-role-in-critical-infrastructure

ICS trainings, education

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

- OT Railway Cybersecurity (OTCS)

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

ICS conferences

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

Virtual IoT and OT Security Summit

The Virtual Summit: IoT & OT Security Summit will delve into the complexities of securing IoT and OT environments. Featuring industry luminaries, this summit offers keynotes, case-based learning and roundtable discussions tailored to address the latest threats and best practices in cyber risk management, zero trust networks, and critical infrastructure protection. Attendees will gain actionable insights on topics such as IT and OT convergence, manufacturing cybersecurity frameworks, and supply chain security, fostering a comprehensive understanding of the evolving cyber landscape.

Virtual, online; 5th December 2024

More details can be found on the following website:

https://ismg.events/summit/virtual-it-ot-2024/

Operational Technology Security Webinar Series 2024

Digital transformation is driving the modernization of industrial infrastructures increasing the integration between operational technology (OT) systems and internet-connected information technology (IT). This evolution has rapidly expanded the attack surface and increased the complexity that operations leaders face when managing their systems.

Virtual, online; 5th December 2024

More details can be found on the following website:

https://events.fortinet.com/otwebinars2024/home

ICS incidents

Texas-based oilfield services hit by ransomware

In late October 2024, Texas-based oilfield services company Newpark Resources detected a ransomware attack in which an unauthorized third party gained access to parts of the company's internal systems. The breach led Newpark to activate its cybersecurity response plan, immediately enlisting internal teams and external advisors to investigate and contain the threat. Although the attack temporarily disrupted access to some information systems and business applications crucial for financial reporting and corporate functions, the company managed to continue essential manufacturing and field operations by implementing established downtime protocols.

The company disclosed the incident in a filing with the U.S. Securities and Exchange Commission (SEC), noting that the financial impact remains uncertain. Newpark's leadership believes that, based on current information, the incident is unlikely to have a significant impact on the company's financial standing or operational results. However, should circumstances change, the company has pledged to provide updates as needed.

This incident at Newpark follows a similar case at Halliburton, a global oilfield services company that suffered a cyberattack in August. Halliburton's response included system shutdowns and activating a cybersecurity response plan. The company reported financial impacts due to lost or delayed revenue, attributing a $0.02 per share reduction in earnings partly to the attack. Halliburton recorded a $116 million pre-tax charge covering severance costs, asset impairment, and cybersecurity incident expenses, illustrating the costly repercussions such breaches can have.

Industry analysts view these incidents as indicative of rising cybersecurity risks within the energy sector, highlighting the importance of transparent incident disclosures required under SEC guidelines. Andy Watkin-Child, a governance, risk, and compliance expert, noted that such transparency reflects the growing awareness of cybersecurity threats at the corporate board level. As companies become more open about the impacts of cyber incidents, it reinforces the priority of cybersecurity in organizational risk management and response planning across critical infrastructure industries.

The source is available on the following link:

https://industrialcyber.co/utilities-energy-power-water-waste/newpark-resources-hit-by-ransomware-activates-cybersecurity-response/

Book recommendation

Operational Technology: A Holistic View

Dive into the comprehensive guide on Operational Technology (OT), penned by an industry expert. In a world where digital transformation is redefining industries, understanding OT's multifaceted role is paramount.

Contents:

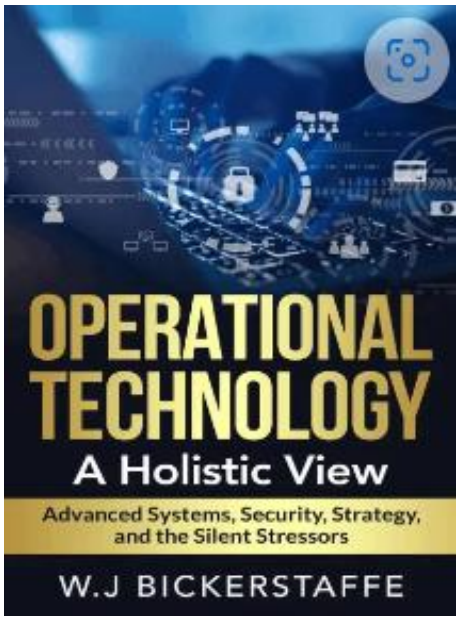
- Chapter 1 - Brushing Up on Foundational Concepts
- Chapter 2 - Unpacking Control Systems
- Chapter 3 - Emerging Technologies in OT
- Chapter 4 - Remote Operations Centres
- Chapter 5 - Communication Protocols
- Chapter 6 - Advanced Security in OT Systems
- Chapter 7 - IT/OT Integration
- Chapter 8 - The Human Touch in OT
- Chapter 9 - Looking Beyond the Horizon

Author/Editor: W.J Bickerstaffe

Year of issue: 2023

The book is available at the following link:

https://www.everand.com/book/667340097/Operational-Technology-A-Holistic-View



ICS security news selection

USDA, ONCD, NRWA launch initiative to bolster cybersecurity in rural water systems

U.S. Department of Agriculture (USDA) has teamed with the White House Office of the National Cyber Director (ONCD) and the National Rural Water Association (NRWA) to strengthen cybersecurity for rural water systems. The agencies will launch a one-year program study to enhance cybersecurity for rural water systems.

Additionally, USDA Rural Development Under Secretary Basil Gooden mentioned that the Oregon Association of Water Utilities and Vermont Rural Water Association will help NRWA administer the one-year study. …

Source and more information:

https://industrialcyber.co/news/usda-oncd-nrwa-launch-initiative-to-bolster-cybersecurity-in-rural-water-systems/

Industrial companies in Europe targeted with GuLoader

A recent spear-phishing campaign targeting industrial and engineering companies in Europe was aimed at saddling victims with the popular GuLoader downloader and, ultimately, a remote access trojan that would permit attackers to steal information from and access compromised computers whenever they wish.

"The emails are sent from various email addresses including from fake companies and compromised accounts. The emails typically hijack an existing email thread or request information about an order," Tara Gould, Threat Research Lead at Cado Security, has warned. …

Source and more information:

https://www.helpnetsecurity.com/2024/11/07/industrial-europe-spear-phishing-guloader/

Can Automatic Updates for Critical Infrastructure Be Trusted?

In July, the industry witnessed one of the largest technology outages in recent history, with estimates of $5.4 billion in damages. When CrowdStrike distributed a Rapid Response Content Channel Update with an exception-handling logic flaw, it opened

the door for constructive conversations about automatic updates — when to use them, when not to use them, whether they make us more or less secure. It's time to reflect and ask: What is the cost of our relentless pursuit of innovation, software currency, and speed to market? How can we reprioritize to reestablish the balance in the C-I-A triad? …

Source and more information:

https://www.darkreading.com/vulnerabilities-threats/can-automatic-updates-critical-infrastructure-be-trusted

ACSC's OT Cyber Security Principles: Call to action for critical infrastructure providers to boost cyber resilience

After releasing guidelines to help critical infrastructure providers effectively secure and protect their operational technology (OT) systems, the Australian Signals Directorate's Australian Cyber Security Centre told organizations that provide critical infrastructure to use the principles to inform the design, implementation, and management of IT ecosystems and the supply chains that support such essential services. The initiative is expected to help prevent cyber threats and address risks that could be potentially faced. …

Source and more information:

https://industrialcyber.co/features/acscs-ot-cyber-security-principles-call-to-action-for-critical-infrastructure-providers-to-boost-cyber-resilience/

DOE's CESER launches ICS cybersecurity training initiative to bolster energy sector workforce strategy

As part of a larger effort to strengthen its cybersecurity workforce strategy, the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) announced Wednesday that it is accepting submissions for its State of Industrial Control System Cybersecurity (ICS) Training opportunity. The effort will fund market research to better understand the ICS and operational technology (OT) cybersecurity workforce landscape and future needs in the energy sector. …

Source and more information:

https://industrialcyber.co/utilities-energy-power-water-waste/does-ceser-launches-ics-cybersecurity-training-initiative-to-bolster-energy-sector-workforce-strategy/

Leaky Cybersecurity Holes Put Water Systems at Risk

At least 97 major water systems in the US have serious cybersecurity vulnerabilities and compliance issues, raising concerns that cyberattacks could disrupt businesses, industry, and the lives of millions of citizens.

Despite a spate of recent cyberattacks raising the awareness of water-infrastructure vulnerabilities, nearly 100 large community water systems (CWS) continue to have serious security weaknesses in Internet-facing systems, putting the water supply of nearly 27 million Americans at risk. …

Source and more information:

https://www.darkreading.com/vulnerabilities-threats/leaky-cybersecurity-holes-water-systems-risk

145,000 Systems Exposed to Web, Many Industrial Firms Hit by Attacks

Worldwide there are more than 145,000 internet-exposed industrial control systems (ICS), according to internet intelligence platform provider Censys.

The company's latest 'State of the Internet' report also reveals that the devices are spread out across 175 countries, with 38% of them located in North America, 35% in Europe and 22% in Asia.

In the United States, there are 48,000 exposed systems. Censys previously reported seeing 40,000 internet-exposed ICS systems in the United States. …

Source and more information:

https://www.securityweek.com/ics-security-145000-systems-exposed-to-web-many-industrial-firms-hit-by-attacks/

Australia's Cyber Defense report highlights evolving threats and strategic countermeasures

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) recently published the 2023–24 Annual Cyber Threat Report outlining the cyber threat posed to the country's governments, critical infrastructure, businesses, and household installations. It shows how malicious state actors and cybercriminals are evolving tactics to breach Australian networks. It underscores the critical need for robust public-private partnerships to protect Australians from cyber threats and strengthen national defenses. It also details the decisive actions being taken to deter and hold

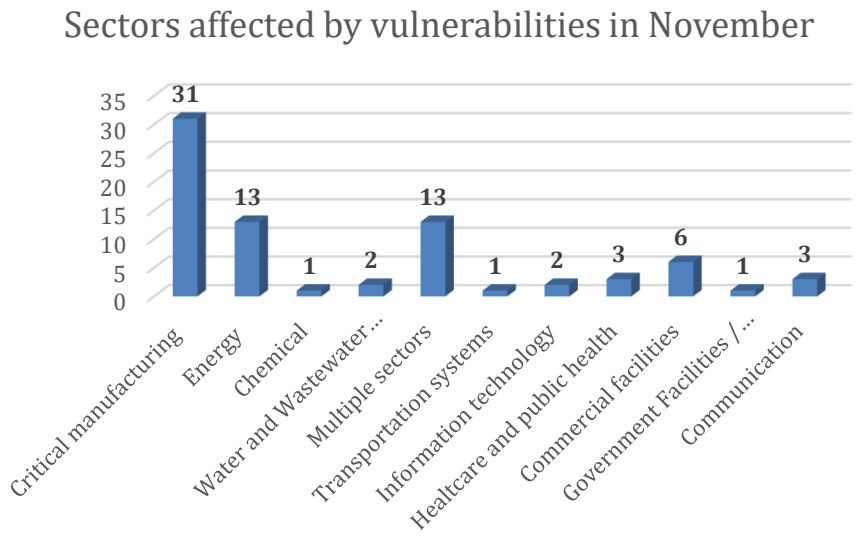
cybercriminals accountable, including the Government's inaugural use of Australia's autonomous cyber sanctions framework to impose sanctions on Russian cybercriminals. …

Source and more information:

https://industrialcyber.co/reports/australias-cyber-defense-report-highlights-evolving-threats-and-strategic-countermeasures/

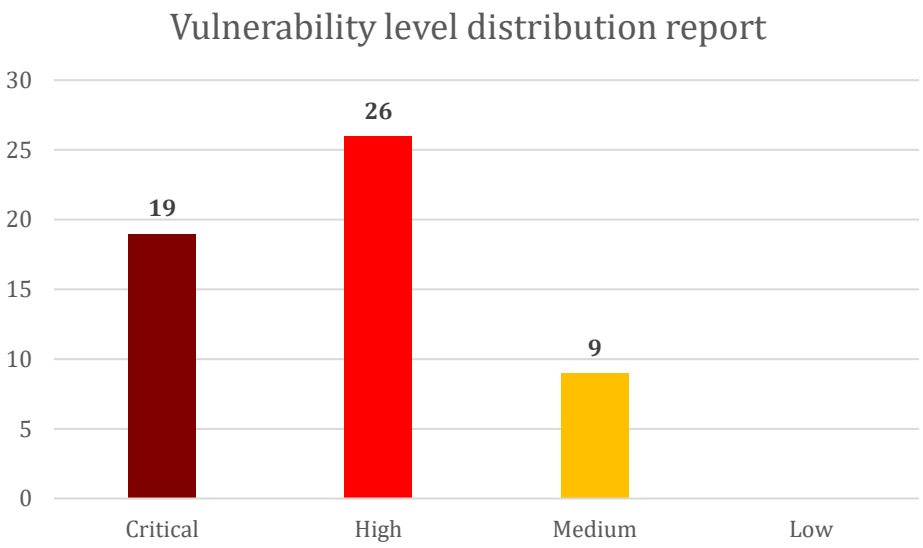
ICS vulnerabilities

In November 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 November:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	10
Out-of-bounds Read	CWE-125	6
Uncontrolled Resource Consumption	CWE-400	6
Missing Authentication for Critical Function	CWE-306	6



ICSA-24-331-01: **Schneider Electric PowerLogic PM55xx and PowerLogic PM8ECC**

Critical level vulnerabilities: Weak Password Recovery Mechanism for Forgotten Password, Improper Authentication.

Schneider Electric PowerLogic PM55xx and PowerLogic PM8ECC | CISA

ICSA-24-331-02: **Schneider Electric PowerLogic P5**

Medium level vulnerability: Use of a Broken or Risky Cryptographic Algorithm.

Schneider Electric PowerLogic P5 | CISA

ICSA-24-331-03: **Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs**

High level vulnerabilities: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Use of Hard-coded Credentials, Insufficiently Protected Credentials.

Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs | CISA

ICSA-24-331-04: **Hitachi Energy MicroSCADA Pro/X SYS600**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Data Query Logic, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Authentication Bypass by Capture-replay, Missing Authentication for Critical Function, URL Redirection to Untrusted Site ('Open Redirect').

Hitachi Energy MicroSCADA Pro/X SYS600 | CISA

ICSA-24-331-05: **Hitachi Energy RTU500 Scripting Interface**

High level vulnerability: Improper Certificate Validation.

Hitachi Energy RTU500 Scripting Interface | CISA

ICSMA-24-200-01: **Philips Vue PACS (Update A)**

Medium level vulnerabilities: Allocation of Resources Without Limits or Throttling, Use of Default Credentials.

Philips Vue PACS (Update A) | CISA

ICSA-24-326-01: **Automated Logic WebCTRL Premium Server**

Critical level vulnerabilities: Unrestricted Upload of File with Dangerous Type, URL Redirection to Untrusted Site ('Open Redirect').

Automated Logic WebCTRL Premium Server | CISA

ICSA-24-326-02: **OSCAT Basic Library**

Medium level vulnerability: Out-of-bounds Read.

OSCAT Basic Library | CISA

ICSA-24-326-03: **Schneider Electric Modicon M340, MC80, and Momentum Unity M1E** **High** level vulnerabilities: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Authentication Bypass by Spoofing.

Schneider Electric Modicon M340, MC80, and Momentum Unity M1E | CISA

ICSA-24-326-04: **Schneider Electric Modicon M340, MC80, and Momentum Unity M1E** **Critical** level vulnerabilities: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Schneider Electric Modicon M340, MC80, and Momentum Unity M1E | CISA

ICSA-24-326-05: **Schneider Electric EcoStruxure IT Gateway**

Critical level vulnerability: Missing Authorization.

Schneider Electric EcoStruxure IT Gateway | CISA

ICSA-24-326-06: **Schneider Electric PowerLogic PM5300 Series**

High level vulnerability: Uncontrolled Resource Consumption.

Schneider Electric PowerLogic PM5300 Series | CISA

ICSA-24-326-07: **mySCADA myPRO Manager**

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

mySCADA myPRO Manager | CISA

ICSA-24-324-01: **Mitsubishi Electric MELSEC iQ-F Series**

High level vulnerability: Improper Validation of Specified Type of Input.

Mitsubishi Electric MELSEC iQ-F Series | CISA

ICSA-24-319-01: **Siemens RUGGEDCOM CROSSBOW**

Medium level vulnerabilities: Heap-based Buffer Overflow, Use After Free.

Siemens RUGGEDCOM CROSSBOW | CISA

ICSA-24-319-02: **Siemens SIPORT**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SIPORT | CISA

ICSA-24-319-03: **Siemens OZW672 and OZW772 Web Server**

High level vulnerability: Cross-site Scripting.

Siemens OZW672 and OZW772 Web Server | CISA

ICSA-24-319-04: **Siemens SINEC NMS**

High level vulnerabilities: Improper Input Validation, Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Write, Uncontrolled Resource Consumption, HTTP Request/Response Splitting, Missing Encryption of Sensitive Data, Out-of-bounds Read, Improper Certificate Validation, Missing Release of Resource after Effective Lifetime, Improper Validation of Certificate with Host Mismatch, Allocation of Resources Without Limits or Throttling, Incorrect Permission Assignment for Critical Resource.

Siemens SINEC NMS | CISA

ICSA-24-319-05: **Siemens Solid Edge**

High level vulnerabilities: Out-of-bounds Read, Uncontrolled Search Path Element.

Siemens Solid Edge | CISA

ICSA-24-319-06: **Siemens SCALANCE M-800 Family**

High level vulnerabilities: Out-of-bounds Read, Missing Encryption of Sensitive Data, Integer Overflow or Wraparound, Uncontrolled Resource Consumption, Excessive Iteration, Use After Free, Improper Output Neutralization for Logs, Observable Discrepancy, Improper Locking, Missing Release of Resource after Effective Lifetime, Improper Input Validation, Improper Access Control, Path Traversal, Cross-site Scripting, Injection.

Siemens SCALANCE M-800 Family | CISA

ICSA-24-319-07: **Siemens Engineering Platforms**

High level vulnerability: Deserialization of Untrusted Data.

Siemens Engineering Platforms | CISA

ICSA-24-319-08: **Siemens SINEC INS**

Critical level vulnerabilities: Improper Authentication, Out-of-bounds Write, Inefficient Regular Expression Complexity, Excessive Iteration, Reachable Assertion, Uncontrolled Resource Consumption, Improper Input Validation, Improper Check for Unusual or Exceptional Conditions, Memory Allocation with Excessive Size Value, Heap-based Buffer Overflow, Missing Encryption of Sensitive Data, Path Traversal, Incorrect Permission Assignment for Critical Resource, Exposure of Sensitive Information to an Unauthorized Actor, Covert Timing Channel, Truncation of Security-relevant Information, Integer Overflow or Wraparound, Use After Free, Code Injection, Path Traversal: 'dir/../../filename', Execution with Unnecessary Privileges, Server-Side Request Forgery (SSRF), OS Command Injection, HTTP Request/Response Smuggling, Use of Hard-coded Cryptographic Key, Insufficient Session Expiration.

Siemens SINEC INS | CISA

ICSA-24-319-09: **Siemens Spectrum Power 7**

High level vulnerability: Incorrect Privilege Assignment.

Siemens Spectrum Power 7 | CISA

ICSA-24-319-10: **Siemens TeleControl Server**

Critical level vulnerability: Deserialization of Untrusted Data.

Siemens TeleControl Server | CISA

ICSA-24-319-11: **Siemens SIMATIC CP**

High level vulnerability: Incorrect Authorization.

Siemens SIMATIC CP | CISA

ICSA-24-319-12: **Siemens Mendix Runtime**

Medium level vulnerability: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition').

Siemens Mendix Runtime | CISA

ICSA-24-319-13: **Rockwell Automation Verve Asset Manager**

High level vulnerability: Dependency on Vulnerable Third-Party Component.

Rockwell Automation Verve Asset Manager | CISA

ICSA-24-319-14: **Rockwell Automation FactoryTalk Updater**

Critical level vulnerabilities: Insecure Storage of Sensitive Information, Improper Input Validation, Improperly Implemented Security Check for Standard.

Rockwell Automation FactoryTalk Updater | CISA

ICSA-24-319-15: **Rockwell Automation Arena Input Analyzer**

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

Rockwell Automation Arena Input Analyzer | CISA

ICSA-24-319-16: **Hitachi Energy MSM**

High level vulnerabilities: Missing Release of Resource after Effective Lifetime, Loop with Unreachable Exit Condition ('Infinite Loop').

Hitachi Energy MSM | CISA

ICSA-24-319-17: **2N Access Commander**

High level vulnerabilities: Path Traversal, Insufficient Verification of Data Authenticity.

2N Access Commander | CISA

ICSA-24-291-01: **Elvaco M-Bus Metering Gateway CMe3100 (Update A)**

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 (Update A) | CISA

ICSMA-24-319-01: **Baxter Life2000 Ventilation System**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Improper Restriction of Excessive Authentication Attempts, Use of Hard-Coded Credentials, Improper Physical Access Control, Download of Code Without Integrity Check, On-Chip Debug and Test Interface With Improper Access Control, Missing Support for Security Features in On-Chip Fabrics or Buses, Missing Authentication for Critical Function, Insufficient Logging.

Baxter Life2000 Ventilation System | CISA

SSA-962515: **Siemens Industrial Products (Update: 1.4)**

High level vulnerability: Out-of-bounds Read.

SSA-962515

SSA-883918: **Siemens SIMATIC WinCC (Update: 1.2)**

High level vulnerability: Exposure of Private Personal Information to an Unauthorized Actor.

SSA-883918

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.1)**

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

SSA-876787

SSA-773256: **Siemens Industrial Products (Update: 1.1)**

Medium level vulnerability: Improper Input Validation.

SSA-773256

SSA-723487: **Siemens SCALANCE, RUGGEDCOM and Related Products (Update: 1.2)** **Critical** level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-629254: **Siemens SIMATIC SCADA and PCS 7 systems (Update: 1.2)**

Critical level vulnerability: Execution with Unnecessary Privileges.

SSA-629254

SSA-599968: **Siemens Profinet Devices (Update: 1.7)**

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

SSA-599968

SSA-398330: **GNU/Linux subsystem of the SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update: 2.0)**

Critical level vulnerabilities: Multiple.

SSA-398330

SSA-364175: **Palo Alto Networks Virtual NGFW on Siemens RUGGEDCOM APE1808 Devices Before V11.1.4-h1 (Update: 1.3)**

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

SSA-364175

SSA-265688: **GNU/Linux subsystem of the Siemens SIMATIC S7-1500 TM MFP V1.1 (Update: 1.3)**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Out-of-bounds Read, Use After Free, Out-of-bounds Write, Improper Input Validation, Uncontrolled Resource Consumption, Exposure of Sensitive Information to an Unauthorized Actor.

SSA-265688

SSA-097435: **Siemens Mendix Runtime (Update: 1.4)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435

SSA-054046: **Web Server of Siemens SIMATIC S7-1500 CPUs (Update: 1.1)**

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

SSA-054046

SSA-039007: **Siemens User Management Component (UMC) (Update: 1.2)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-039007

ICSA-24-317-01: **Subnet Solutions PowerSYSTEM Center**

Critical level vulnerabilities: Improper Restriction of XML External Entity Reference, Integer Overflow or Wraparound.

Subnet Solutions PowerSYSTEM Center | CISA

ICSA-24-317-02: **Hitachi Energy TRO600**

High level vulnerabilities: Command Injection, Improper Removal of Sensitive Information Before Storage or Transfer.

Hitachi Energy TRO600 | CISA

ICSA-24-317-03: **Rockwell Automation FactoryTalk View ME**

High level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk View ME | CISA

ICSA-23-306-03: **Mitsubishi Electric MELSEC Series (Update A)**

Critical level vulnerability: Missing Authentication for Critical Function.

Mitsubishi Electric MELSEC Series (Update A) | CISA

ICSA-23-136-01: **Snap One OvrC Cloud (Update A)**

Critical level vulnerabilities: Improper Input Validation, Observable Response Discrepancy, Improper Access Control, Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity, Open Redirect, Use of Hard-coded Credentials, Hidden Functionality, Authentication Bypass by Spoofing, Missing Authentication for Critical Function.

Snap One OvrC Cloud (Update A) | CISA

ICSA-24-312-01: **Beckhoff Automation TwinCAT Package Manager**

High level vulnerability: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Beckhoff Automation TwinCAT Package Manager | CISA

ICSA-24-312-02: **Delta Electronics DIAScreen**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics DIAScreen | CISA

ICSA-24-312-03: **Bosch Rexroth IndraDrive**

High level vulnerability: Uncontrolled Resource Consumption.

Bosch Rexroth IndraDrive | 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 November:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-8957 PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability;
CVE-2024-8956 PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability;
CVE-2024-43093 Android Framework Privilege Escalation Vulnerability;
CVE-2024-51567 CyberPanel Incorrect Default Permissions Vulnerability;
CVE-2019-16278 Nostromo nhttpd Directory Traversal Vulnerability;
CVE-2024-5910 Palo Alto Expedition Missing Authentication Vulnerability;
CVE-2021-26086 Atlassian Jira Server and Data Center Path Traversal Vulnerability;
CVE-2014-2120 Cisco Adaptive Security Appliance (ASA) Cross-Site Scripting (XSS) Vulnerability;
CVE-2021-41277 Metabase GeoJSON API Local File Inclusion Vulnerability;
CVE-2024-43451 Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability;
CVE-2024-49039 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability;
CVE-2024-9463 Palo Alto Networks Expedition OS Command Injection Vulnerability;
CVE-2024-9465 Palo Alto Networks Expedition SQL Injection Vulnerability;
CVE-2024-1212 Progress Kemp LoadMaster OS Command Injection Vulnerability;
CVE-2024-0012 Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability;
CVE-2024-9474 Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability;
CVE-2024-38812 VMware vCenter Server Heap-Based Buffer Overflow Vulnerability;
CVE-2024-38813 VMware vCenter Server Privilege Escalation Vulnerability;
CVE-2024-44308 Apple Multiple Products Code Execution Vulnerability;
CVE-2024-44309 Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability;
CVE-2024-21287 Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability;
CVE-2023-28461 Array Networks AG and vxAG ArrayOS Improper Authentication Vulnerability;
Links and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two 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, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities

Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and international partners released joint Cybersecurity Advisory, 2023 Top Routinely Exploited Vulnerabilities.

Links and more information:

CISA, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities | CISA

Citrix Releases Security Updates for NetScaler and Citrix Session Recording

Citrix released security updates to address multiple vulnerabilities in NetScaler ADC, NetScaler Gateway, and Citrix Session Recording. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Citrix Releases Security Updates for NetScaler and Citrix Session Recording | CISA

JCDC's Collaborative Efforts Enhance Cybersecurity for the 2024 Olympic and Paralympic Games

The Cybersecurity and Infrastructure Security Agency (CISA), through the Joint Cyber Defense Collaborative (JCDC), enabled proactive coordination and information sharing to bolster cybersecurity ahead of the 2024 Olympic and Paralympic Games in Paris. Recognizing the potential for cyber threats targeting the Games, CISA worked to strengthen U.S. private sector ties and facilitate connections with key French counterparts to promote collective defense measures.

Links and more information:

JCDC's Collaborative Efforts Enhance Cybersecurity for the 2024 Olympic and Paralympic Games | CISA

Ivanti Releases Security Updates for Multiple Products

Ivanti released security updates to address vulnerabilities in Ivanti Endpoint Manager (EPM), Ivanti Avalanche, Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Security Access Client.

Links and more information:

Ivanti Releases Security Updates for Multiple Products | 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

Microsoft Releases November 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 November 2024 Security Updates | CISA

Fortinet Releases Security Updates for Multiple Products

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

Links and more information:

Fortinet Releases Security Updates for Multiple Products | CISA

Palo Alto Networks Emphasizes Hardening Guidance

Palo Alto Networks (PAN) has released an important informational bulletin on securing management interfaces after becoming aware of claims of an unverified remote code execution vulnerability via the PAN-OS management interface.

Links and more information:

Palo Alto Networks Emphasizes Hardening Guidance | CISA

USDA Releases Success Story Detailing the Implementation of Phishing-Resistant Multi-Factor Authentication

Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Agriculture (USDA) released Phishing-Resistant Multi-Factor Authentication (MFA) Success Story: USDA's FIDO Implementation. This report details how USDA successfully implemented phishing-resistant authentication for its personnel in situations where USDA could not exclusively rely on personal identity verification (PIV) cards.

Links and more information:

USDA Releases Success Story Detailing the Implementation of Phishing-Resistant Multi-Factor Authentication | CISA

CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory

CISA, the Federal Bureau of Investigation (FBI), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released updates to #StopRansomware: BianLian Ransomware Group on observed tactics, techniques, and procedures (TTPs) and indicators of compromise attributed to data extortion group, BianLian.

Links and more information:

CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory | CISA

2024 CWE Top 25 Most Dangerous Software Weaknesses

The Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the Homeland Security Systems Engineering and Development Institute (HSSEDI), operated by MITRE, has released the 2024 CWE Top 25 Most Dangerous Software Weaknesses. This annual list identifies the most critical software weaknesses that adversaries frequently exploit to compromise systems, steal sensitive data, or disrupt essential services.

Links and more information:

2024 CWE Top 25 Most Dangerous Software Weaknesses | CISA

Apple Releases Security Updates for Multiple Products

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

Links and more information:

Apple Releases Security Updates for Multiple Products | CISA

CISA Releases Insights from Red Team Assessment of a U.S. Critical Infrastructure Sector Organization

CISA released Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization in coordination with the assessed organization. This cybersecurity advisory details lessons learned and key findings from an assessment, including the Red Team's tactics, techniques, and procedures (TTPs) and associated network defense activity.

Links and more information:

CISA Releases Insights from Red Team Assessment of a U.S. Critical Infrastructure Sector Organization | CISA