2024 July, 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

Cybersecurity Best Practices in the Manufacturing Sector

The Industrialcyber website has published a webinar and its content description on its website, showcasing best practices for cybersecurity in the manufacturing sector. The webinar link is available on the website, and the following topics are covered in it:

- Understanding the Complexity of Manufacturing Cybersecurity
  - Manufacturing Environments and Cybersecurity Challenges
- The Role of Visibility in Cybersecurity
- Evolving Role of the CISO in Manufacturing
  - From Technician to Diplomat: The CISO's Journey
  - Best Practices for Fostering Collaboration
- Engaging Stakeholders and Securing Buy-In
  - Building a Compelling Business Case for Cybersecurity
  - Leveraging Regulatory Compliance for Stakeholder Engagement
- Building Awareness
  - Promoting Cybersecurity Awareness & Reducing Threats
  - Increasing Productivity by Engaging Stakeholders
  - Increasing Efficacy and Saving on Cost
  - Increasing Flexibility and Adaptation in Deployment
- Measuring the Value of Cybersecurity Investments
  - Cyber Insurance as a Benchmark
- Embracing Digital Transformation with Cybersecurity

Questions and answers related to the above topics are also described, which may arise. It is advisable to review these as well and assess their relevance to the organization.

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

https://industrialcyber.co/manufacturing/cybersecurity-best-practices-in-the-manufacturing-sector/?_gl=1*1e7nq89*_up*MQ..*_ga*MTc3OTM0NTU4LjE3MTkzOTIwMjk.*_ga_T2BXH1VHY7*MTcxOTgxNDA2NC40LjAuMTcxOTgxNDA2NC4wLjAuMA..

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in August 2024:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

- Industrial Control System (ICS) & SCADA Cyber Security Training

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

- ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

- NIST(800-82) Industrial Control system(ICS) Security

https://www.udemy.com/course/nist800-82-industrial-control-systemics-security/

- ICS/OT Cybersecurity All in One as per NIST Standards

https://www.udemy.com/course/ics-cybersecurity/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

https://www.infosectrain.com/operational-technology-ot-training-courses/#courses

ICS conferences

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

7th International Symposium for Industrial Control System & SCADA Cyber Security Research

The 7th International Symposium for ICS & SCADA Cyber Security brings together researchers with an interest in the security of industrial control systems in the light of their increasing exposure to cyber-space. The topics of interests are broad, ranging from security for hardware/firmware used in industrial control systems, to system aspects of ICS such as secure architectures and vulnerability screening to the human aspects of cyber security such as behaviour modelling and training. ICS-CSR is a research conference aimed at high quality academic research in any of the specified themes and topics of interest. We welcome original contributions that present innovative ideas, proof of concepts, use cases, and results from a variety of domains with a wish to enhance the security of infrastructure.

Vienna, Austria; 1st August 2024

More details can be found on the following website:

https://sites.google.com/view/ics-csr/

ISA/IEC 62443 Cybersecurity Fundamentals Specialist 2024

Virtual workshop with the following themes:

- Discuss the principles behind creating an effective long term program security
- Interpret the ISA/IEC 62443 industrial security framework and apply them to your operation
- Define the basics of risk and vulnerability analysis methodologies
- Describe the principles of security policy development
- Explain the concepts of defense in depth and zone/conduit models of security

Virtual; 5th – 8th August 2024

More details can be found on the following website:

https://10times.com/e1xr-fkd0-340x

ICS incidents

Forklift Manufacturer Halts Operations to Investigate Cyberattack

One of the largest forklift manufacturers has been compelled to shut down its operational systems following a significant cyberattack.

Crown Equipment announced that it experienced a cyberattack and is currently investigating the incident, attributing the attack to an unnamed "international cybercriminal organization."

The company, a major player in the defense industry with over $4 billion in revenue last year, is collaborating with federal law enforcement to determine the next steps.

"The company is still working through the disruption caused by the attack and is making progress toward transitioning to normal business operations," Crown Equipment stated.

"Crown is also working closely with its customers to help reduce the effect the incident may have on their operations."

The Ohio-based company employs nearly 20,000 people across about 24 plants worldwide.

The news outlet Born City reported that Crown Equipment has faced significant operational disruption since June 8, dealing with a ransomware attack. Employees have voiced their frustrations in the comment sections of news stories and on Reddit about the lack of information from Crown.

Hourly workers have also experienced pay losses since operations at the company's factories have come to a standstill. Some workers have been advised to file for unemployment insurance while the company attempts to restore its operations.

Bleeping Computer obtained an email sent to employees on Tuesday, indicating that the attack originated from an employee who "failed to adhere to our data security policies by allowing unauthorized access to their device."

The source is available on the following link:

https://therecord.media/crown-equipment-shuts-down-systems-forklifts

Book recommendation

Strengthening Industrial Cybersecurity to Protect Business Intelligence

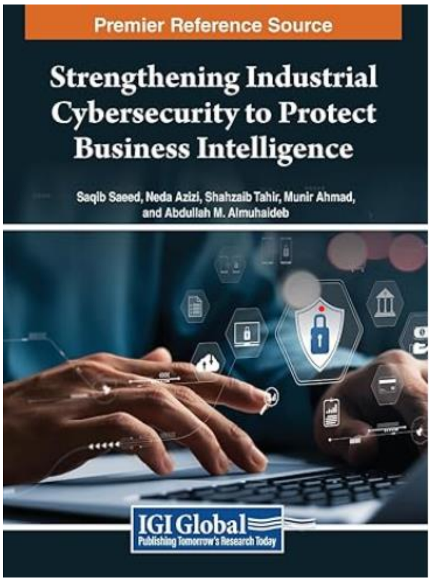
In the digital transformation era, integrating business intelligence and data analytics has become critical for the growth and sustainability of industrial organizations. However, with this technological evolution comes the pressing need for robust cybersecurity measures to safeguard valuable business intelligence from security threats. Strengthening Industrial Cybersecurity to Protect Business Intelligence delves into the theoretical foundations and empirical studies surrounding the intersection of business intelligence and cybersecurity within various industrial domains. This book addresses the importance of cybersecurity controls in mitigating financial losses and reputational damage caused by cyber-attacks. The content spans a spectrum of topics, including advances in business intelligence, the role of artificial intelligence in various business applications, and the integration of intelligent systems across industry 5.0. Ideal for academics in information systems, cybersecurity, and organizational science, as well as government officials and organizations, this book serves as a vital resource for understanding the intricate relationship between business intelligence and cybersecurity. It is equally beneficial for students seeking insights into the security implications of digital transformation processes for achieving business continuity.

Author/Editor: Saqib Saeed (Editor), Neda Azizi (Editor), Shahzaib Tahir (Editor)

Year of issue: 2024

The book is available at the following link:

https://www.amazon.com/Strengthening-Industrial-Cybersecurity-Business-Intelligence/dp/B0CPQ47PP8


Premier Reference Source
Strengthening Industrial Cybersecurity to Protect Business Intelligence
Saqib Saeed, Neda Azizi, Shahzaib Tahir, Munir Ahmad, and Abdullah M. Almuhaideb
IGI Global
Publishing Tomorrow's Research Today

ICS security news selection

Gas Chromatograph Hacking Could Have Serious Impact: Security Firm

Claroty, a company that specializes in security solutions for cyber-physical systems, has disclosed the details of several vulnerabilities discovered in a gas chromatograph made by Emerson, and warned that attacks could have a serious impact.

A gas chromatograph is a chemical analysis instrument that measures the content of various components in a sample. Such devices are used by hospitals in blood testing and by environmental facilities to measure air pollution. …

Source and more information:

https://www.securityweek.com/gas-chromatograph-hacking-could-have-serious-impact-security-firm/

Australian CISC details submission window for CIRMP Annual Report, cybersecurity framework compliance

Having come to the end of the Australian financial year 2023-2024, the nation’s Cyber and Infrastructure Security Centre (CISC) outlined that the Critical Infrastructure Risk Management Program (CIRMP) Annual Report for this period should be submitted between July 1, 2024, and Sept. 28, 2024, using the Responsible Entity Risk Management Program – Annual Report Form. Additionally, by Aug. 17, 2024, responsible entities are required to establish and maintain a cybersecurity framework under Section 8 of the Security of Critical Infrastructure (SOCI) CIRMP Rules. …

Source and more information:

https://industrialcyber.co/regulation-standards-and-compliance/australian-cisc-details-submission-window-for-cirmp-annual-report-cybersecurity-framework-compliance/?_gl=1*1bfzu0e*_up*MQ..*_ga*MjAzMDgyOTk5MC4xNzIwMTcwNzU2*_ga_T2BXH1VHY7*MTcyMDE3MDc1My4xLjAuMTcyMDE3MDc1My4wLjAuMA..

Equipping Students and Educators with Industrial Cybersecurity Knowledge

Cybersecurity events such as Volt Typhoon and a wave of ransomware attacks have drawn unprecedented attention to the need for cybersecurity in industrial control system environments. At a fundamental level, the solution depends on developing qualified and prepared professionals capable of operating seamlessly in cybersecurity and engineering, IT and OT.

To establish a foundation for meeting this need, the ISA Global Cybersecurity Alliance (ISAGCA), together with Idaho State University, the Idaho National Laboratory and the U.S. Department of Energy Office of Cybersecurity, Energy Security and Emergency Response, has released the Curricular Guidance: Industrial Cybersecurity Knowledge document. …

Source and more information:

https://www.automation.com/en-us/articles/july-2024/students-educators-industrial-cybersecurity

Growing need to safeguard industrial systems with effective OT cybersecurity programs

Evolving cyber threats and attacks underscore the critical need for effective OT cybersecurity programs to protect industrial systems and infrastructure. Unlike traditional IT systems, OT (operational technology) environments comprise hardware and software that make detections or changes, and they do this by directly monitoring and controlling physical devices, processes, and events. Due to this, organizations must construct and build an effective OT cybersecurity program that considers several unique challenges pulled from legacy systems, real-time operational needs, safety-critical functions, and others. …

Source and more information:

https://industrialcyber.co/features/growing-need-to-safeguard-industrial-systems-with-effective-ot-cybersecurity-programs/?_gl=1*klo136*_up*MQ..*_ga*MTYxNzE2Nzg0MC4xNzIwNTE1NDA0*_ga_T2BXH1VHY7*MTcyMDUxNTQwMS4xLjAuMTcyMDUxNTQwMS42MC4wLjA.

Defending OT Requires Agility, Proactive Controls

As attackers set their sights on infrastructure, security teams need to reduce risk levels without compromising operational agility.

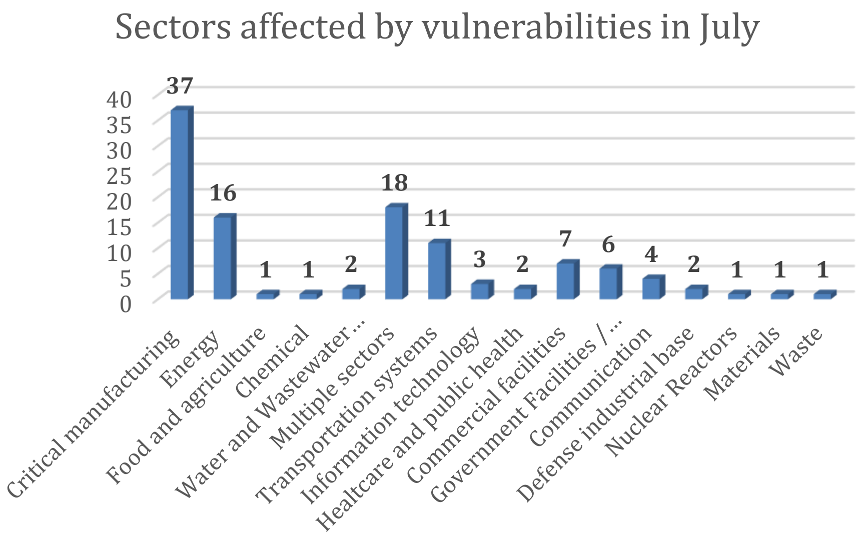
Hackers affiliated with the Chinese government have reportedly maintained access to US critical infrastructure for years, several agencies warned in February. The revelation is, at least on the surface, a heel-turn for Chinese cyber behaviour — moving from espionage to the potential compromise or destruction of infrastructure via operational technology (OT). This includes the programmable systems and devices connected to physical environments. …

Source and more information:

https://www.darkreading.com/ics-ot-security/defending-ot-requires-agility-proactive-controls

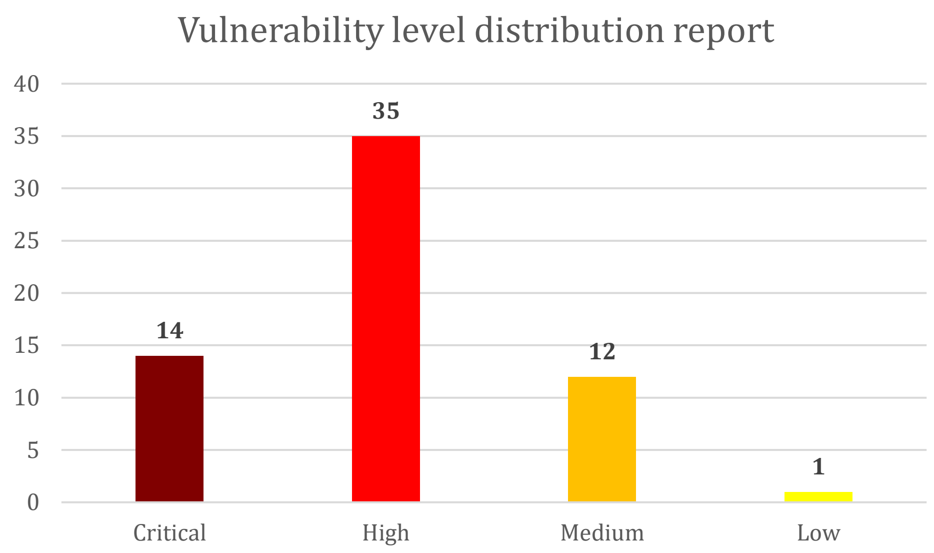
ICS vulnerabilities

In July 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 July:

Vulnerability	CWE number	Items
Uncontrolled Resource Consumption	CWE-400	7
Out-of-bounds Read	CWE-125	5
Stack-based Buffer Overflow	CWE-121	5



ICSA-24-207-01: **Siemens SICAM Products**

Critical level vulnerabilities: Unverified Password Change, Missing Authentication for Critical Function.

[Siemens SICAM Products | CISA]

ICSA-24-207-02: **Positron Broadcast Signal Processor**

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

[Positron Broadcast Signal Processor | CISA]

ICSA-24-205-01: **National Instruments IO Trace**

High level vulnerability: Stack-Based Buffer Overflow.

[National Instruments IO Trace | CISA]

ICSA-24-205-02: **Hitachi Energy AFS/AFR Series Products**

High level vulnerabilities: Type Confusion, Use After Free, Double Free, Observable Discrepancy.

[Hitachi Energy AFS/AFR Series Products | CISA]

ICSA-24-205-03: **National Instruments LabVIEW**

High level vulnerabilities: Out-of-Bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer.

[National Instruments LabVIEW | CISA]

ICSA-22-333-02: **Hitachi Energy IED Connectivity Packages and PCM600 Products (Update A)**

High level vulnerability: Cleartext Storage of Sensitive Information.

Hitachi Energy IED Connectivity Packages and PCM600 Products (Update A) | CISA

ICSA-24-200-01: **Mitsubishi Electric MELSOFT MaiLab**

High level vulnerability: Improper Verification of Cryptographic Signature.

Mitsubishi Electric MELSOFT MaiLab | CISA

ICSA-24-200-02: **Subnet Solutions PowerSYSTEM Center**

Medium level vulnerability: Prototype Pollution.

Subnet Solutions PowerSYSTEM Center | CISA

ICSMA-24-200-01: **Philips Vue PACS**

Critical level vulnerabilities: Out-of-bounds Write, Deserialization of Untrusted Data, Uncontrolled Resource Consumption, Improper Privilege Management, Use of Default Credentials, Weak Password Requirements, Exposure of Sensitive Information to an Unauthorized Actor.

Philips Vue PACS | CISA

ICSA-24-198-01: **Rockwell Automation Pavilion 8**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Rockwell Automation Pavilion 8 | CISA

SSA-981975: **Siemens SIMATIC IPCs (Update: 1.2.)**

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

SSA-981975 (siemens.com)

SSA-962515: **Siemens Industrial Products (Update: 1.1.)**

High level vulnerability: Out-of-bounds Read.

SSA-962515 (siemens.com)

SSA-832273: **Siemens RUGGEDCOM APE1808 devices (Update: 1.4.)**

Critical level vulnerabilities: Multiple.

SSA-832273 (siemens.com)

SSA-780073: **Siemens PROFINET Devices via DCE-RPC Packets (Update: 2.4.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-780073 (siemens.com)

SSA-753746: **Siemens SIMATIC WinCC Affecting Other SIMATIC Software Products (Update: 1.3.)**

High level vulnerability: NULL Pointer Dereference.

SSA-753746 (siemens.com)

SSA-750274: **Siemens RUGGEDCOM APE1808 devices configured with Palo Alto Networks Virtual NGFW (Update: 1.1.)**

Critical level vulnerability: Improper Neutralization of Special Elements used in a Command ('Command Injection').

SSA-750274 (siemens.com)

SSA-730482: **Siemens SIMATIC WinCC (Update: 1.1.)**

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

SSA-730482 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update: 2.8.)**

High level vulnerability: Loop with Unreachable Exit Condition ('Infinite Loop').

SSA-712929 (siemens.com)

SSA-686975: **Siemens Siemens Industrial Products using Intel CPUs (Update: 1.4.)**

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

SSA-686975 (siemens.com)

SSA-593272: **Siemens Industrial Devices (Update: 2.2.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-593272 (siemens.com)

SSA-484086: **Siemens SINEMA Remote Connect Server before V3.1 (Update: 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-484086 (siemens.com)

SSA-473245: **Siemens Profinet Devices (Update: 2.7.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-473245 (siemens.com)

SSA-455250: **Siemens RUGGEDCOM APE1808 devices before V11.1.2-h3 (Update: 1.2.)** **Critical** level vulnerabilities: Multiple.

SSA-455250 (siemens.com)

SSA-446448: **Siemens PROFINET Stack Integrated on Interniche Stack (Update: 2.2.)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

SSA-446448 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update: 1.1.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-346262: **Siemens SNMP Interface of Industrial Products (Update: 3.3.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-346262 (siemens.com)

SSA-337522: **Siemens TIM 1531 IRC before V2.4.8 (Update: 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-337522 (siemens.com)

SSA-293562: **Siemens Industrial Products (Update: 3.5.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-293562 (siemens.com)

SSA-265688: **Siemens SIMATIC S7-1500 TM MFP V1.1 (Update: 1.2.)**

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

SSA-265688 (siemens.com)

SSA-160243: **Siemens SINEC NMS before V2.0 (Update: 1.1.)**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

SSA-160243 (siemens.com)

ICSA-24-193-01: **Siemens Remote Connect Server**

Critical level vulnerabilities: Incorrect User Management, Unrestricted Upload of File with Dangerous Type, Forced Browsing, Improper Check for Unusual or Exceptional Conditions, Client-Side Enforcement of Server-Side Security, Incorrect Authorization, Creation of Temporary File With Insecure Permissions, Improper Restriction of Excessive Authentication Attempts, Incorrect Permission Assignment for Critical Resource, Allocation of Resources Without Limits or Throttling.

Siemens Remote Connect Server | CISA

ICSA-24-193-02: **Siemens RUGGEDCOM APE 1808**

High level vulnerabilities: Stack-based Buffer Overflow, Use of Password Hash With Insufficient Computational Effort, Cross-site Scripting.

Siemens RUGGEDCOM APE 1808 | CISA

ICSA-24-193-03: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerability: Out-of-bounds Read.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-193-04: **Siemens Simcenter Femap**

High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write, Type Confusion, Improper Restriction of Operations within the Bounds of a Memory Buffer, Stack-based Buffer Overflow.

Siemens Simcenter Femap | CISA

ICSA-24-193-05: **Siemens SCALANCE, RUGGEDCOM, SIPLUS, and SINEC**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Siemens SCALANCE, RUGGEDCOM, SIPLUS, and SINEC | CISA

ICSA-24-193-06: **Siemens RUGGEDCOM**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Incorrect Privilege Assignment, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Siemens RUGGEDCOM | CISA

ICSA-24-193-07: **Siemens SIMATIC and SIMIT**

Medium level vulnerability: Improperly Controlled Sequential Memory Allocation.

Siemens SIMATIC and SIMIT | CISA

ICSA-24-193-08: **Siemens Mendix Encryption Module**

High level vulnerability: Use of Hard-coded, Security-relevant Constants.

Siemens Mendix Encryption Module | CISA

ICSA-24-193-09: **Siemens SINEMA Remote Connect Server**

High level vulnerability: Command Injection.

Siemens SINEMA Remote Connect Server | CISA

ICSA-24-193-10: **Siemens JT Open and PLM XML SDK**

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

Siemens JT Open and PLM XML SDK | CISA

ICSA-24-193-11: **Siemens RUGGEDCOM APE 1808**

High level vulnerability: Truncation of Security-relevant Information.

Siemens RUGGEDCOM APE 1808 | CISA

ICSA-24-193-12: **Siemens TIA Portal and SIMATIC STEP 7**

High level vulnerability: Deserialization of Untrusted Data.

Siemens TIA Portal and SIMATIC STEP 7 | CISA

ICSA-24-193-13: **Siemens TIA Portal, SIMATIC, and SIRIUS**

High level vulnerability: Deserialization of Untrusted Data.

Siemens TIA Portal, SIMATIC, and SIRIUS | CISA

ICSA-24-193-14: **Siemens SIPROTEC**

Medium level vulnerability: Inadequate Encryption Strength.

Siemens SIPROTEC | CISA

ICSA-24-193-15: **Siemens SINEMA Remote Connect Server**

High level vulnerability: Command Injection.

Siemens SINEMA Remote Connect Server | CISA

ICSA-24-193-16: **Siemens SIMATIC WinCC**

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

Siemens SIMATIC WinCC | CISA

ICSA-24-193-17: **Siemens SIMATIC STEP 7 (TIA Portal)**

High level vulnerability: Deserialization of Untrusted Data.

Siemens SIMATIC STEP 7 (TIA Portal) | CISA

ICSA-24-193-18: **Rockwell Automation ThinManager ThinServer**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation ThinManager ThinServer | CISA

ICSA-24-193-19: **Rockwell Automation FactoryTalk System Services and Policy Manager**

Medium level vulnerability: Improper Privilege Management.

Rockwell Automation FactoryTalk System Services and Policy Manager | CISA

ICSA-24-193-20: **HMS Industrial Networks Anybus-CompactCom 30**

Medium level vulnerability: Cross-site Scripting.

HMS Industrial Networks Anybus-CompactCom 30 | CISA

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

High level vulnerability: Improper Resource Shutdown or Release.

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

ICSA-24-191-01: **Delta Electronics CNCSoft-G2**

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

Delta Electronics CNCSoft-G2 | CISA

ICSA-24-191-02: **Mitsubishi Electric MELIPC Series MI5122-VW**

High level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric MELIPC Series MI5122-VW | CISA

ICSA-24-191-03: **Johnson Controls Illustra Pro Gen 4**

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

Johnson Controls Illustra Pro Gen 4 | CISA

ICSA-24-191-04: **Johnson Controls Software House C•CURE 9000**

High level vulnerability: Use of Weak Credentials.

Johnson Controls Software House C•CURE 9000 | CISA

ICSA-24-191-05: **Johnson Controls Software House C•CURE 9000**

High level vulnerability: Incorrect Default Permissions.

Johnson Controls Software House C•CURE 9000 | CISA

ICSA-24-177-02: **PTC Creo Elements/Direct License Server (Update A)**

Critical level vulnerability: Missing Authorization.

PTC Creo Elements/Direct License Server (Update A) | CISA

ICSA-23-269-03: **Mitsubishi Electric FA Engineering Software (Update A)**

Critical level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric FA Engineering Software (Update A) | CISA

ICSA-24-184-01: **Johnson Controls Kantech Door Controllers**

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

Johnson Controls Kantech Door Controllers | CISA

ICSA-24-184-02: **mySCADA myPRO**

Critical level vulnerability: Use of Hard-coded Password.

mySCADA myPRO | CISA

ICSA-24-184-03: **ICONICS and Mitsubishi Electric Products**

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

ICONICS and Mitsubishi Electric Products | CISA

ICSA-24-179-04: **Johnson Controls Illustra Essentials Gen 4 (Update A)**

Critical level vulnerability: Improper Input Validation.

Johnson Controls Illustra Essentials Gen 4 (Update A) | CISA

ICSA-24-179-05: **Johnson Controls Illustra Essentials Gen 4 (Update A)**

Medium level vulnerability: Storing Passwords in a Recoverable Format.

Johnson Controls Illustra Essentials Gen 4 (Update A) | CISA

ICSA-24-179-06: **Johnson Controls Illustra Essentials Gen 4 (Update A)**

Medium level vulnerability: Insertion of Sensitive Information into Log File.

Johnson Controls Illustra Essentials Gen 4 (Update A) | CISA

ICSA-24-179-07: **Johnson Controls Illustra Essentials Gen 4 (Update A)**

Medium level vulnerability: Storing Passwords in a Recoverable Format.

Johnson Controls Illustra Essentials Gen 4 (Update A) | CISA

The vulnerability reports contain more detailed information, which can be found on the following websites:

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

CISA has published alerts in 2024 July:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-20399 Cisco NX-OS Command Injection Vulnerability;
CVE-2024-23692 Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability;
CVE-2024-38080 Microsoft Windows Hyper-V Privilege Escalation Vulnerability;
CVE-2024-38112 Microsoft Windows MSHTML Platform Spoofing Vulnerability;
CVE-2024-36401 OSGeo GeoServer GeoTools Eval Injection Vulnerability;
CVE-2024-34102 Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability;
CVE-2024-28995 SolarWinds Serv-U Path Traversal Vulnerability;
CVE-2022-22948 VMware vCenter Server Incorrect Default File Permissions Vulnerability;
CVE-2012-4792 Microsoft Internet Explorer Use-After-Free Vulnerability;
CVE-2024-39891 Twilio Authy Information Disclosure Vulnerability;
CVE-2024-4879 ServiceNow Improper Input Validation Vulnerability;
CVE-2024-5217 ServiceNow Incomplete List of Disallowed Inputs Vulnerability;
CVE-2023-45249 Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability;
CVE-2024-37085 VMware ESXi Authentication Bypass Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability 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

Juniper Networks Releases Security Bulletin for Junos OS: SRX Series
Juniper Networks released a security bulletin to address a vulnerability in Junos OS: SRX Series. A cyber threat actor could exploit this vulnerability to cause a denial-of-service condition.
Links and more information:
Juniper Networks Releases Security Bulletin for Junos OS: SRX Series | CISA

CISA and Partners join ASD'S ACSC to Release Advisory on PRC State-Sponsored Group, APT 40

CISA has collaborated with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) to release an advisory, People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action outlining a PRC state-sponsored cyber group's activity.

Links and more information:
CISA and Partners join ASD'S ACSC to Release Advisory on PRC State-Sponsored Group, APT 40 | CISA

Microsoft Releases July 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 July 2024 Security Updates | CISA

Citrix Releases Security Updates for Multiple Products

Citrix released security updates to address vulnerabilities in multiple Citrix products. 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 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

CISA and FBI Release Secure by Design Alert on Eliminating OS Command Injection Vulnerabilities

CISA and FBI are releasing their newest Secure by Design Alert in the series, Eliminating OS Command Injection Vulnerabilities, in response to recent well-publicized threat actor campaigns that exploited OS command injection defects in network edge devices (CVE-2024-20399, CVE-2024-3400, CVE-2024-21887) to target and compromise users. These *vulnerabilities allowed unauthenticated malicious actors to remotely execute code on network edge devices.*

Links and more information:
CISA and FBI Release Secure by Design Alert on Eliminating OS Command Injection Vulnerabilities | CISA

CISA Releases Advisory Detailing Red Team Activity During Assessment of US FCEB Organization, Highlighting Necessity of Defense-in-Depth

CISA released CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth in coordination with the assessed organization. This Cybersecurity Advisory (CSA) details key findings and lessons learned from a 2023 assessment, along with the red team's tactics, techniques, and procedures (TTPs) and associated network defense activity.

Links and more information:
CISA Releases Advisory Detailing Red Team Activity During Assessment of US FCEB Organization, Highlighting Necessity of Defense-in-Depth | CISA

AT&T Discloses Breach of Customer Data

On July 12, AT&T released a public statement on unauthorized access of customer data from a third-party cloud platform. AT&T also provided recommendations and resources for affected customers.

Links and more information:
AT&T Discloses Breach of Customer Data | CISA

Oracle Releases Critical Patch Update Advisory for July 2024

Oracle released its quarterly Critical Patch Update Advisory for July 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 Critical Patch Update Advisory for July 2024 | CISA

Ivanti Releases Security Updates for Endpoint Manager

Ivanti released security updates to address vulnerabilities in Ivanti Endpoint Manager (EPM) and Ivanti Endpoint Manager for Mobile (EPMM). A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:
Ivanti Releases Security Updates for Endpoint Manager | CISA

Cisco Releases Security Updates for Multiple Products

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

Links and more information:

Cisco Releases Security Updates for Multiple Products | CISA

ISC Releases Security Advisories for BIND 9

The Internet Systems Consortium (ISC) released security advisories to address vulnerabilities affecting multiple versions of ISC's Berkeley Internet Name Domain (BIND) 9. A cyber threat actor could exploit one of these vulnerabilities to cause a denial-of-service condition.

Links and more information:

ISC Releases Security Advisories for BIND 9 | CISA

FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity

CISA—in partnership with the Federal Bureau of Investigation (FBI)—released a joint Cybersecurity Advisory, North Korea State-Sponsored Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs.

Links and more information:

FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity | CISA

Apple Releases Security Updates for Multiple Products

Apple released security updates to address vulnerabilities in Safari, iOS, iPadOS, macOS, watchOS, tvOS, and visionOS. 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

DigiCert Certificate Revocations

DigiCert, a certificate authority (CA) organization, is revoking a subset of transport layer security (TLS) certificates due to a non-compliance issue with domain control verification (DCV). Revocation of these certificates may cause temporary disruptions to websites, services, and applications relying on these certificates for secure communication.

DigiCert has notified affected customers and provided instructions on how to replace non-compliant certificates.

Links and more information:

DigiCert Certificate Revocations | CISA