2024 February, 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, 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

Available Podcasts from 2023 on the following link.

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

- Ep. 38: Xavier Mesrobian on the Microsoft DCOM hardening patch
- Ep. 39: Dom Lombardi on Mobile Device Management
- Ep. 40: Xavier Mesrobian on SCADA Security

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

Industrial Defender

- Podcast: The PrOtect OT Cybersecurity Podcast: 2023 Wrapped

Link: The PrOtect OT Cybersecurity Podcast: 2023 Wrapped | Industrial Defender OT/ICS Cybersecurity Blog

ICS Cyber Talks Podcast

- Shimi Cohen, the CISO of UBTECH, an ethical hacker and Cyber threat intelligence expert, the founder of "Shimi's Cyber world" and "Hacker Republic" communities, talking about the cyber warfare in Israel since October 7th.
- Alexander Tartakovsky the founder and CEO of iOT365 OT Cyber Security Platform delivered as a SAAS. We discussed changing the mindset for traditional and innovative OT infrastructure as part of Industry 4.0, Open PLC, and digital twin technologies.

Link: https://icscybertalks.podbean.com/

BEERISAC: OT/ICS Security Podcast Playlist

- Managing Trust in Massive IIoT Systems [The Industrial Security Podcast]
- David Elfering on CISOs and Cyber Liability Insurance
- Cyber Physical Security As A Shared Responsibility
- Cybersecurity in Rail Operations: A CISO's Triumphs, Challenges, and Lessons Learned
- Talking Cyber. Hackers Cause Water Outage In Ireland. Heather Engel, Strategic Cyber Partners
- Juan Piacquadio on Securing Pharma 4.0
- A free community initiative to protect small utilities
- Cyber Life Podcast Ep. 26 - Critical Infrastructure Cybersecurity with Chip Harris
- OT or IT with Consequences – with John Burns
- Cybersecurity in the Power Grid – A 360° View | Part 5
- How the Merck Case Shapes the Future of Cyber Insurance
- USB Firmware Attacks [The Industrial Security Podcast]
- Beyond Boundaries: Unveiling the Multifaceted World of Michelle Balderson
- Why Mapping IT Security to OT Networks Doesn't Always Work
- Henning Kruse: When OT, Network Security and Automotive Meet
- Feeding the Digital Age: Unpacking Cyber Risks (Part 1)
- Cyber Av3ngers and their unlikely targets
- OT Security Made Simple | OT-Sicherheit aus Sicht eines Pentesters
- OT Security Made Simple | The 4 types of OT monitoring and which to choose
- Building community in OT
- Team82 Answers More of your OT Cybersecurity Questions
- World Peace still Requires Changing Default Passwords with Marty Edwards
- What's Next? A decision support tool for industrial security [The Industrial Security Podcast]

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/

ICS good practices, recommendations

Online ransomware decryptor helps recover partially encrypted files

CyberArk has launched an online version of 'White Phoenix,' an open-source ransomware decryptor designed to assist victims of intermittent encryption attacks. In response to the growing threat of ransomware, CyberArk aims to provide accessible solutions for those affected, particularly individuals less familiar with technical coding.

White Phoenix is a user-friendly tool available online, allowing victims to easily upload files and initiate the recovery process with the click of a button. The tool supports various file formats including PDFs, Word documents, Excel sheets, ZIP files, and PowerPoint presentations, with a file size limit of 10MB. For larger files or virtual machines, the GitHub version is recommended.

Many ransomware operations, including Blackcat/ALPHV, Play, Qilin/Agenda, BianLian, and DarkBit, utilize intermittent encryption to expedite attacks. While this method accelerates the encryption process, it often leaves portions of files unencrypted, presenting an opportunity for restoration.

White Phoenix employs sophisticated techniques to reconstruct files, focusing on concatenating unencrypted segments and reversing hex encoding and character mapping scrambling. While its effectiveness may vary depending on the ransomware strain and file type, White Phoenix serves as an automated tool inspired by manual restoration methods used by data recovery experts.

It's essential to note that White Phoenix may not guarantee full system restoration but can potentially retrieve valuable data from compromised files. As there are currently no working decryptors available for the mentioned ransomware families, White Phoenix provides a viable restoration option worth exploring.

If handling sensitive information, we recommend downloading White Phoenix from GitHub and utilizing it locally to maintain confidentiality. While our online platform ensures accessibility, safeguarding privacy remains a priority.

Source, and more information available on the following link:

https://www.bleepingcomputer.com/news/security/online-ransomware-decryptor-helps-recover-partially-encrypted-files/

ICS trainings, education

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

ICS conferences

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

Critical Infrastructure Protection & Resilience North America

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

Lake Charles, Louisiana, USA; 12th -14th March 2024

More details can be found on the following website:

https://ciprna-expo.com/

SmartGrid Tech Week 2024

The conference focused on the implementation of lessons learnt from the integration of the latest digital technologies into traditional grid domains. This meeting provides the entire smart grid technical team with the opportunity to gather the latest grid innovation intelligence, scout for the latest innovations, and network with like-minded peers from across Europe, facing the same digital transformation pressure and priorities.

With 70+ utility case-studies scheduled over 3 days, this meeting is the most important date in the calendar for smart grid technical professional charged with digital grid transformation.

Noordwijk, The Netherlands; 18th - 22nd March 2024

More details can be found on the following website:

https://www.smartgrid-forums.com/sgtech-week

CS4CA USA Summit

As critical infrastructure continues its transition from analog to digital, the surface for cyber attacks has expanded and the resulting risks to an organization's physical assets, people, financial liability, and reputation are increasing in frequency and potency.

With this in mind, the Cyber Security for Critical Assets Summit brings together senior cybersecurity leaders from across US critical infrastructure, for 2-days of in-depth knowledge exchange, strategy planning and insight building.

This is a unique opportunity to build partnerships with senior cybersecurity executives from the country's Oil & Gas, Energy, Utilities, Power, Water, Mining, Chemical and Transportation industries while participating in the discussions shaping the American cybersecurity landscape in 2024 and beyond.

Houston, Texas, USA; 26th – 27th March 2024

More details can be found on the following website:

https://usa.cs4ca.com/?gad_source=1&gclid=Cj0KCQiAn-2tBhDVARIsAGmStVkD1Sv7jZRc2whpfzsr40JB21aIoWNmp7emsWNKPZANXqYoLcgZInsaAg4WEALw_wcB

ICS incidents

Veolia North America and Southern Water hit by ransomware attacks

Industrialcyber reported incidents which affected Veolia North America and Southern Water in the UK. Both companies experienced ransomware attacks affecting certain software applications and systems. Veolia responded swiftly, taking targeted systems offline and implementing defensive measures. While some customers faced delays in online bill payments, normal operations have since resumed. Veolia assured customers that late payments due to the incident won't incur penalties.

The breach at Veolia seems to have been contained within its internal systems, with no evidence of impact on water or wastewater treatment operations. However, a limited number of individuals' personal information may have been compromised, and Veolia is contacting them directly to provide assistance. The company is conducting a thorough investigation with a third-party forensics firm to prevent such incidents in the future.

Similarly, Southern Water detected suspicious activity and initiated an investigation, though there's no evidence of impact on customer relationships or financial systems. They've informed relevant authorities and are following cybersecurity advice closely. Reports suggest the Black Basta ransomware group claimed responsibility, potentially exposing personal data and HR-related documents.

Experts emphasize the importance of securing operational technology (OT) systems, although neither company's OT systems were reportedly disrupted. They advise organizations, especially in critical sectors like water and wastewater, to incorporate cybersecurity best practices outlined in recent guidance from agencies like CISA, FBI, and EPA. The Southern Water breach highlights the risks posed by modern corporate structures and supply chains, with implications for data security and protection across subsidiaries and suppliers. The water industry's vulnerability to cyber threats underscores the need for enhanced cybersecurity measures in critical sectors.

The source is available on the following link:

https://industrialcyber.co/utilities-energy-power-water-waste/veolia-north-america-and-southern-water-hit-by-ransomware-attacks-data-breach-concerns-arise/

Book recommendation

Engineering-Grade OT Security: A manager's guide

Imagine you work in a power plant that uses a half dozen massive, 5-story-tall steam boilers. If a cyber-attack makes a boiler over-pressurize and explode, the event will most likely kill you and everyone else nearby. Which mitigation for that risk would you prefer? A mechanical over-pressure valve on each boiler where, if the pressure in the boiler gets too high, then the steam forces the valve open, the steam escapes, and the pressure is released? Or a longer password on the computer controlling the boilers?

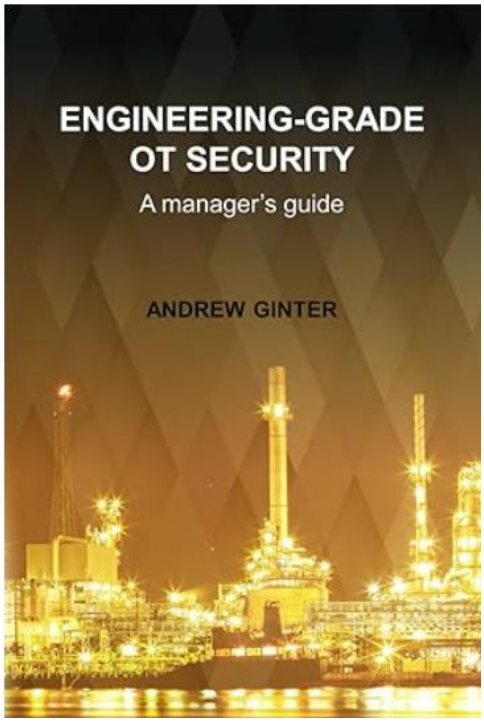
Addressing cyber risks to physical operations takes more than cybersecurity. The engineering profession has managed physical risks and threats to safety and public safety for over a century. Process, automation and network engineering are powerful tools to address OT cyber risks - tools that simply do not exist in the IT domain. This text explores these tools, explores risk and looks at what "due care" means in today's changing cyber threat landscape.

Author/Editor: Andrew Ginter (Author)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/Engineering-Grade-OT-Security-managers-guide/dp/B0CJLLN9WW



ICS security news selection

Zero trust implementation: Plan, then execute, one step at a time

82% of cybersecurity professionals have been working on implementing zero trust last year, and 16% should be on it by the end of this year.

The challenges of zero trust implementation

You've probably heard it before: zero trust is not a single product, but a security strategy that follows the principle of "never trust, always verify". As such, it requires a customized approach, which can be quite complicated and might require additional staff.

Implementing zero trust means an overall change in technology and architecture, and doing it one step at the time. Legacy systems that were not designed to operate within a zero-trust framework might require different security measures or possibly require replacement, resulting in additional expenses. …

Source and more information:

https://www.helpnetsecurity.com/2024/02/01/zero-trust-challenges/

OT Maintenance Is Primary Source of OT Security Incidents: Report

A recent report from TXOne Networks, a Taiwan-based cybersecurity firm focusing on operational technology (OT), looks at OT security incidents and their sources, as well as the preparedness of organizations against attacks.

The report is based on a combination of data from a survey of over 400 CIOs conducted in September 2023 by Frost & Sullivan, and data collected by TXOne itself from more than 500 incidents that occurred last year in North America, Europe and the APAC region. The survey respondents represented organizations in the United States, Germany, Japan and the United Arab Emirates (UAE), with roughly 100 respondents from each country. …

Source and more information:

https://www.securityweek.com/ot-maintenance-is-primary-source-of-ot-security-incidents-report/

Executive Order on Port Cybersecurity Points to IT/OT Threat Posed by Chinese Cranes

The White House announced on Wednesday that the Biden-Harris administration is issuing an executive order to boost the cybersecurity of US ports, highlighting the risks posed by the use of cranes made by China.

Ports, vessels, shipping companies, and other entities in the maritime sector are regularly impacted by cyber incidents, as shown by the maritime cyberattack database launched last year by a Dutch University. Studies have shown that many incidents involve operational technology (OT) systems.

Experts have warned that vulnerabilities in the IT and OT systems used in the maritime industry can pose a significant threat to supply chains and the global economy. …

Source and more information:

https://www.securityweek.com/executive-order-on-port-cybersecurity-points-to-it-ot-threat-posed-by-chinese-cranes/

Russian hacker is set to face trial for the hack of a local power grid

The news agency TASS reported that a Russian national (49) is set to face trial on charges of carrying out a cyberattack on a local power plant that left 38 villages in the Vologda region in the dark.

The attack took place one year ago, the man faces up to eight years in prison.

"The criminal investigation has been completed against a hacker who cut off power to 38 settlements in the Vologda region. The Russian FSB Directorate for the Vologda Region established that in February 2023, a resident of the region born in 1975 gained unlawful access to technological control systems for power grids and cut off power to 38 settlements Vologda region in the Sheksninsky district, Ustyuzhensky and Babayevsky districts," the press service of the Russian FSB department for the Vologda region told TASS. …

Source and more information:

https://securityaffairs.com/159536/hacking/cyber-attack-power-plant-russia-hacker.html

NIST CSF 2.0 released, to help all organizations, not just those in critical infrastructure

The National Institute of Standards and Technology (NIST) has updated its widely utilized Cybersecurity Framework (CSF), a key document for mitigating cybersecurity risks. The latest version, 2.0, is tailored to cater to a broad range of audiences, spanning various industry sectors and organizational sizes – from small schools and non-profits to major agencies and corporations. This update is relevant for all, irrespective of their level of expertise in cybersecurity.

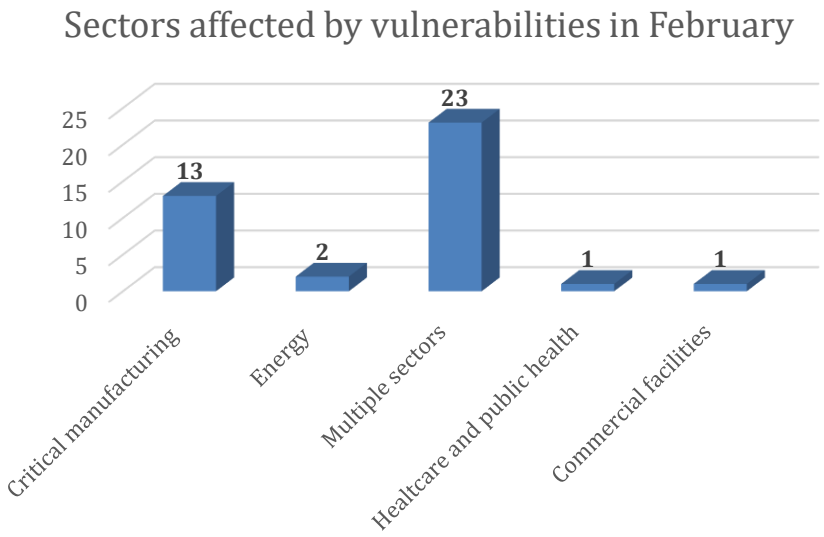
NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to implement. …

Source and more information:

https://www.helpnetsecurity.com/2024/02/27/nist-csf-2-released/

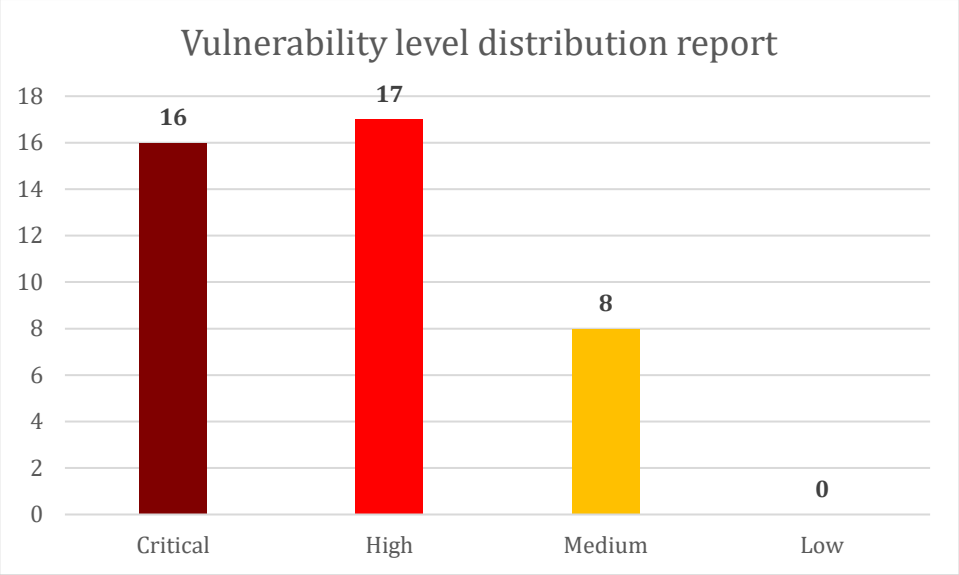
ICS vulnerabilities

In February 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 February:

Vulnerability	CWE number	Items
NULL Pointer Dereference	CWE-476	6
Improper Input Validation	CWE-20	6
Out-of-bounds Read	CWE-125	6
Improper Authentication	CWE-287	3
Cross-site Scripting	CWE-79	3
Path Traversal	CWE-22	3
Out-of-bounds Write	CWE-787	3



ICSA-24-058-01: **Mitsubishi Electric Multiple Factory Automation Products**

Medium level vulnerability: Insufficient Resource Pool.

Mitsubishi Electric Multiple Factory Automation Products | CISA

ICSMA-24-058-01: **Santesoft Sante DICOM Viewer Pro**

High level vulnerability: Out-of-Bounds Read.

Santesoft Sante DICOM Viewer Pro | CISA

ICSA-24-053-01: **Delta Electronics CNCSoft-B DOPSoft**

High level vulnerability: Uncontrolled Search Path Element.

Delta Electronics CNCSoft-B DOPSoft | CISA

ICSA-24-051-01: **Commend WS203VICM**

Critical level vulnerabilities: Argument Injection, Improper Access Control, Weak Encoding for Password.

Commend WS203VICM | CISA

ICSA-24-051-02: **Ethercat Zeek Plugin**

Critical level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read.

Ethercat Zeek Plugin | CISA

ICSA-24-051-03: **Mitsubishi Electric Electrical Discharge Machines**

Critical level vulnerability: Improper Input Validation.

Mitsubishi Electric Electrical Discharge Machines | CISA

ICSA-24-046-01: **Siemens SCALANCE W1750D**

Critical level vulnerabilities: Classic Buffer Overflow, Improper Input Validation, Command Injection.

Siemens SCALANCE W1750D | CISA

ICSA-24-046-02: **Siemens SIDIS Prime**

Critical level vulnerabilities: Use of Insufficiently Random Values, NULL Pointer Dereference, Infinite Loop.

Siemens SIDIS Prime | CISA

ICSA-24-046-03: **Siemens SIMATIC RTLS Gateways**

High level vulnerability: Improper Handling of Length Parameter Inconsistency.

Siemens SIMATIC RTLS Gateways | CISA

ICSA-24-046-04: **Siemens CP343-1 Devices**

High level vulnerability: Improper Verification of Source of a Communication Channel.

Siemens CP343-1 Devices | CISA

ICSA-24-046-05: **Siemens Location Intelligence**

Critical level vulnerability: Use of Hard-coded Credentials.

Siemens Location Intelligence | CISA

ICSA-24-046-06: **Siemens Unicam FX**

High level vulnerability: Incorrect Use of Privileged APIs.

Siemens Unicam FX | CISA

ICSA-24-046-07: **Siemens Tecnomatix Plant Simulation**

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

Siemens Tecnomatix Plant Simulation | CISA

ICSA-24-046-08: **Siemens RUGGEDCOM APE1808**

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

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-046-09: **Siemens SCALANCE SC-600 Family**

Critical level vulnerabilities: Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Weak Hash, Forced Browsing, Uncontrolled Resource Consumption, Unchecked Return Value, Injection, OS Command Injection.

Siemens SCALANCE SC-600 Family | CISA

ICSA-24-046-10: **Siemens Simcenter Femap**

High level vulnerabilities: Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Read, Access of Uninitialized Pointer.

Siemens Simcenter Femap | CISA

ICSA-24-046-11: **Siemens SCALANCE XCM-/XRM-300**

Critical level vulnerabilities: multiple.

Siemens SCALANCE XCM-/XRM-300 | CISA

ICSA-24-046-12: **Siemens SIMATIC WinCC, OpenPCS**

High level vulnerability: NULL Pointer Dereference.

Siemens SIMATIC WinCC, OpenPCS | CISA

ICSA-24-046-13: **Siemens Parasolid**

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

Siemens Parasolid | CISA

ICSA-23-046-14: **Siemens Polarion ALM**

High level vulnerabilities: Incorrect Default Permissions, Improper Authentication.

Siemens Polarion ALM | CISA

ICSA-24-046-15: **Siemens SINEC NMS**

Critical level vulnerabilities: Out-of-bounds Read, Inadequate Encryption Strength, Double Free, Use After Free, NULL Pointer Dereference, Improper Input

Validation, Missing Encryption of Sensitive Data, Allocation of Resources Without Limits or Throttling, Improper Authentication, Inefficient Regular Expression Complexity, Excessive Iteration, HTTP Request/Response Smuggling, Injection, Path Traversal, Race Condition, Improper Certificate Validation, Off-by-one Error, Missing Authorization, Use of Insufficiently Random Values, Buffer Underflow, Incorrect Permission Assignment for Critical Resource, Uncontrolled Resource Consumption, Incorrect Authorization, Type Confusion, Heap-based Buffer Overflow, SQL Injection, Open Redirect, Unrestricted Upload of File with Dangerous Type, OS Command Injection.

Siemens SINEC NMS | CISA

ICSA-24-046-16: **Rockwell Automation FactoryTalk Service Platform**

High level vulnerability: Incorrect Execution-Assigned Permissions.

Rockwell Automation FactoryTalk Service Platform | CISA

ICSA-23-306-02: **Mitsubishi Electric MELSEC iQ-F/iQ-R Series CPU Module (Update A)** **Medium** level vulnerability: Improper Restriction of Excessive Authentication Attempts.

Mitsubishi Electric MELSEC iQ-F/iQ-R Series CPU Module (Update A) | CISA

ICSA-24-044-01: **Mitsubishi Electric MELSEC iQ-R Series Safety CPU**

Medium level vulnerability: Incorrect Privilege Assignment.

Mitsubishi Electric MELSEC iQ-R Series Safety CPU | CISA

SSA-999588: **Siemens User Management Component (UMC) before V2.11.2 (Update: 1.1.)**

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-844761: **Siemens SiNVR/SiVMS Video Server (Update: 1.3.)**

High level vulnerabilities: Cleartext Storage in a File or on Disk, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Input Validation, Inadequate Encryption Strength.

SSA-844761 (siemens.com)

SSA-794697: **Siemens SIMATIC S7-1500 TM MFP V1.0 (Update: 1.6.)**

Critical level vulnerabilities: Multiple.

SSA-794697 (siemens.com)

SSA-772220: **Siemens Industrial Products (Update: 2.3.)**

Medium level vulnerability: NULL Pointer Dereference.

SSA-772220 (siemens.com)

SSA-761844: **Siemens Control Center Server (CCS) (Update: 1.1.)**

Critical level vulnerabilities: Cleartext Storage of Sensitive Information in GUI, Improper Authentication, Relative Path Traversal, Use of a Broken or Risky Cryptographic Algorithm, Exposed Dangerous Method or Function, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Cleartext Storage in a File or on Disk, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Insufficient Logging.

SSA-761844 (siemens.com)

SSA-761617: **Siemens SiNVR/SiVMS Video Server (Update: 1.2.)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Use of a Broken or Risky Cryptographic Algorithm.

SSA-761617 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update: 2.5.)**

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

SSA-712929 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update: 1.4.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-570294: **Siemens SICAM Q100 Before V2.50 (Update: 1.1.)**

Critical level vulnerabilities: Session Fixation, Improper Input Validation.

SSA-570294 (siemens.com)

SSA-480095: **Siemens SICAM Q100 Devices before V2.60 (Update: 1.1.)**

Medium level vulnerabilities: Cross-Site Request Forgery (CSRF), Incorrect Permission Assignment for Critical Resource.

SSA-480095 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU (Update: 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

ICSA-24-039-01: **Qolsys IQ Panel 4, IQ4 HUB**

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

Qolsys IQ Panel 4, IQ4 HUB | CISA

ICSA-23-082-06: **ProPump and Controls Osprey Pump Controller (Update A)**

Critical level vulnerabilities: Insufficient Entropy, Use of GET Request Method with Sensitive Query Strings, Use of Hard-coded Password, OS Command Injection, Cross-site Scripting, Authentication Bypass using an Alternate Path or Channel, Cross-Site Request Forgery, Command Injection.

ProPump and Controls Osprey Pump Controller (Update A) | CISA

ICSA-24-037-01: **HID Global Encoders**

Medium level vulnerability: Improper Authorization.

HID Global Encoders | CISA

ICSA-24-037-02: **HID Global Reader Configuration Cards**

Medium level vulnerability: Improper Authorization.

HID Global Reader Configuration Cards | CISA

ICSA-24-032-01: **Gessler GmbH WEB-MASTER**

Critical level vulnerabilities: Use of Weak Credentials, Use of Weak Hash.

Gessler GmbH WEB-MASTER | CISA

ICSA-24-032-03: **AVEVA Edge products (formerly known as InduSoft Web Studio)**

High level vulnerability: Uncontrolled Search Path Element.

AVEVA Edge products (formerly known as InduSoft Web Studio) | 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 February:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-4762 Google Chromium V8 Type Confusion Vulnerability;
CVE-2024-21762 Fortinet FortiOS Out-of-Bound Write Vulnerability;
CVE-2023-43770 Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability;
CVE-2024-21412 Microsoft Windows Internet Shortcut Files Security Feature Bypass Vulnerability;
CVE-2024-21351 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability;
CVE-2020-3259 Cisco ASA and FTD Information Disclosure Vulnerability;
CVE-2024-21410 Microsoft Exchange Server Privilege Escalation Vulnerability;
CVE-2024-1709 ConnectWise ScreenConnect Authentication Bypass 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 One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Moby and Open Container Initiative Release Critical Updates for Multiple Vulnerabilities Affecting Docker-related Components
Moby and the Open Container Initiative (OCI) have released updates for multiple vulnerabilities (CVE-2024-23651, CVE-2024-23652, CVE-2024-23653, CVE-2024-21626) affecting Docker-related components, including Moby BuildKit and OCI runc. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.
Links and more information:
Moby and Open Container Initiative Release Critical Updates for Multiple Vulnerabilities Affecting Docker-related Components | CISA

Juniper Networks Releases Security Bulletin for Juniper Secure Analytics
Juniper Networks released a security bulletin to address multiple vulnerabilities affecting Juniper Secure Analytics optional applications. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
Juniper Networks Releases Security Bulletin for Juniper Secure Analytics | CISA

VMware Releases Security Advisory for Aria Operations for Networks
VMware released a security advisory to address multiple vulnerabilities in Aria Operations for Networks. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
VMware Releases Security Advisory for Aria Operations for Networks | CISA

CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance
CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure alongside supplemental Joint Guidance: Identifying and Mitigating Living off the Land Techniques.
Links and more information:
CISA and Partners Release Advisory on PRC-sponsored Volt Typhoon Activity and Supplemental Living Off the Land Guidance | CISA

Cisco Releases Security Advisory for Vulnerabilities in Cisco Expressway Series
Cisco released a security advisory to address vulnerabilities affecting Cisco Expressway Series. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
Cisco Releases Security Advisory for Vulnerabilities in Cisco Expressway Series | CISA

CISA Partners With OpenSSF Securing Software Repositories Working Group to Release Principles for Package Repository Security
CISA partnered with the Open Source Security Foundation (OpenSSF) Securing Software Repositories Working Group to publish the Principles for Package Repository Security framework.
Links and more information:
CISA Partners With OpenSSF Securing Software Repositories Working Group to Release Principles for Package Repository Security | CISA

JetBrains Releases Security Advisory for TeamCity On-Premises
JetBrains released a security advisory to address a vulnerability (CVE-2024-23917) in TeamCity On-Premises. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
JetBrains Releases Security Advisory for TeamCity On-Premises | CISA

Fortinet Releases Security Advisories for FortiOS

Fortinet released security updates to address critical remote code execution vulnerabilities in FortiOS (CVE-2024-21762, CVE-2024-23313). A cyber threat actor could exploit these vulnerabilities to take control of an affected system. Note: According to Fortinet, CVE-2024-21762 is potentially being exploited in the wild.

Links and more information:

Fortinet Releases Security Advisories for FortiOS | CISA

Priorities of the Joint Cyber Defense Collaborative for 2024

CISA—on behalf of the collective group of industry and government partners that comprise the Joint Cyber Defense Collaborative (JCDC)—released JCDC's 2024 Priorities.

Links and more information:

Priorities of the Joint Cyber Defense Collaborative for 2024 | 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

Microsoft Releases Security Updates for Multiple Products

Microsoft has 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 Security Updates for Multiple Products | CISA

Adobe Releases Security Updates for Multiple Products

Adobe has released security updates to address 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 MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization

CISA and the Multi-State Information Sharing & Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA), Threat Actor Leverages Compromised Account of Former Employee to Access State Government Organization to provide network defenders with the tactics, techniques, and procedures (TTPs) utilized by a threat actor and methods to protect against similar exploitation.

Links and more information:

CISA and MS-ISAC Release Advisory on Compromised Account Used to Access State Government Organization | CISA

Mozilla Releases Security Updates for Firefox and Thunderbird

Mozilla released security updates to address vulnerabilities in Firefox, Firefox ESR, and Thunderbird. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Mozilla Releases Security Updates for Firefox and Thunderbird | CISA

CISA, EPA, and FBI Release Top Cyber Actions for Securing Water Systems

CISA, the Environmental Protection Agency (EPA), and the Federal Bureau of Investigation (FBI) released the joint fact sheet Top Cyber Actions for Securing Water Systems.

Links and more information:

CISA, EPA, and FBI Release Top Cyber Actions for Securing Water Systems | CISA

Updated: Top Cyber Actions for Securing Water Systems

CISA, the Environmental Protection Agency (EPA), and the Federal Bureau of Investigation (FBI) updated the joint fact sheet Top Cyber Actions for Securing Water Systems.

Links and more information:

Updated: Top Cyber Actions for Securing Water Systems | CISA

CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure

CISA, in partnership with UK National Cyber Security Centre (NCSC) and other U.S. and international partners released the joint advisory, SVR Cyber Actors Adapt Tactics for Initial Cloud Access.

Links and more information:

CISA, NCSC-UK, and Partners Release Advisory on Russian SVR Actors Targeting Cloud Infrastructure | CISA

CISA, FBI, and HHS Release an Update to #StopRansomware Advisory on ALPHV Blackcat

CISA, the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) released an update to the joint advisory #StopRansomware: ALPHV Blackcat to provide new indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the ALPHV Blackcat ransomware as a service (RaaS). ALPHV Blackcat affiliates have been observed primarily targeting the healthcare sector.

Links and more information:

CISA, FBI, and HHS Release an Update to #StopRansomware Advisory on ALPHV Blackcat | CISA

CISA Releases Resource Guide for University Cybersecurity Clinics

CISA released a Resource Guide for Cybersecurity Clinics to outline ways CISA can partner with and support cybersecurity clinics and their clients.

Links and more information:

CISA Releases Resource Guide for University Cybersecurity Clinics | CISA