2024 January, 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.

Check out our new content, the **ICS podcasts**!

List of Contents

ICS podcasts ... 2

ICS good practices, recommendations ... 4

ICS trainings, education ... 5

ICS conferences ... 8

ICS incidents ... 9

Book recommendation ... 10

ICS security news selection ... 11

ICS vulnerabilities ... 14

ICS alerts ... 22

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

- Predictions Analyzed
- Q4 ICS Security Quarter In Review
- CISA Attack Surface Scanning Service

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

Industrial Cybersecurity Pulse

- Ep. 37: Luis Narvaez on bringing SOAR/SOC to OT

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

Industrial Defender

- Podcast: Episode #44 - Thomas VanNorman: ICS Security Takes a Village - Building an OT Security Community

Link: https://www.industrialdefender.com/blog/podcast-episode-44-thomas-vannorman-ics-security-takes-a-village-building-an-ot-security-community

ICS Cyber Talks Podcast

- Alberto Deto Hasson, VP CISO @ICL Group, former Head of National CERT on
- Hadas Tamam Ben-Avraham Cyber crises expert Vice Dean & E-MBA Program

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

BEERISAC: OT/ICS Security Podcast Playlist

- Ep. 39: Dom Lombardi on Mobile Device Management
- EP 26: Securing Railroad OT Systems

- Dining Digitally: Embracing Change Management in Food and Cybersecurity
- OT Cybersecurity: Understanding the Threat, Determining How Much Protection is Enough
- Collaborative Defenses: Strengthening Rail Cybersecurity Together
- Dan Gunter: Lessons Learned from Real-World Attack on Ukraine's Critical Infrastructure
- Robert Smigelski: Where Safety and Security Meet
- Utility attacks and electrical sector supply chain vulnerabilities.
- Ep. 64 - O fim do ICS Security Podcast
- Ep. 38: Xavier Mesrobian on the Microsoft DCOM hardening patch
- Making the Move into OT Security [The Industrial Security Podcast]
- Team82 Answers Your Vulnerability Research Questions
- Digital Transformation – Securing the Future of U.S. Manufacturing
- Andrew Ginter - Illuminating the Path to Industrial Security Excellence with Waterfall Security Solutions

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

ICS good practices, recommendations

2024 Cybersecurity Predictions: Insights From Industry Experts

Global Security Mag has collected predictions for 2024 that will be relevant for industrial cyber defence. Below we present the predictions in a sentence:

- AI will be further adopted by cyber attackers and might see the first AI worm.
- It could also be the year of attackers combining traditional worming ransomware - like WannaCry or notPetya - with more advanced, AI-driven automation to create an aggressive autonomous agent that has sophisticated, context-based decision-making capabilities.
- The emergence of “poly-crisis” due to pervasive AI-based cyber-attacks.
- Microsegmentation will be a foundational element of cyber defense.
- ICS/OT Cybersecurity needs will use AI innovation to solve mundane operational problems.
- As the number of Internet of Things (IoT) devices grows, securing these devices, including OT, will remain a significant concern, with the need for robust security measures and vulnerability management.
- The Zero Trust security model, which assumes zero trust even within an organization, will gain momentum.
- Skill issues will force more hands around AI deployments.
- Education and soft skills will get more focus.
- QR Code Phishing or “quishing” is becoming a very popular form of attack by cybercriminals.
- Apple officially supporting Third party app stores next year in EMEA.
- Regulatory requirements are constantly evolving when it comes to cybersecurity technology, and this will only continue to happen in 2024.
- Another threat to beware of in 2024 is mobile ransomware.
- The growing adoption of application shielding as part of a DevSecOps framework.
- Long-Range Concerns About Nation-States and Even Self-Aware Bots.
- Third-Party Data Sharing Will Raise Risks of Security Breaches.

We strongly recommend thinking about the predictions!

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

https://www.globalsecuritymag.com/2024-Cybersecurity-Predictions-Insights-From-Industry-Experts.html

ICS trainings, education

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

Healthcare & Pharma Virtual Cybersecurity Summit

Don't wait for a breach to happen, take action and safeguard your digital assets now! This is your chance to stay ahead of potential attacks by learning about the latest cybersecurity threats, trends, and solutions at the Healthcare & Pharma Virtual Cybersecurity Conference. Hear from cybersecurity experts and leaders, and connect with other cybersecurity professionals from the region while gaining an edge against nefarious cybersecurity threat actors.

Virtual; 22nd February 2024

More details can be found on the following website:

https://dataconnectors.com/events/2024/healthcare-summit

ManuSec, Cyber Security For Critical Manufacturing Summit

The rapid digitalization of the manufacturing sector has left our organisations open to an increasing number of attacks. Manufacturers have become the top targeted industry by cyberattackers in Europe, with ransomware attacks on industrial infrastructure doubling in 2023. These cyber threats have led our organisations to face an expanded attack surface caused by increased connectivity, with both state sponsored actors and criminal gangs responsible, with attacks heightened in light of Russia's invasion of Ukraine. Consequently, these cyberattacks on the manufacturing industry have far-reaching impacts, affecting operations, supply chains, and ultimately the global economy. Consequently, the 6th Edition of ManuSec Europe will bring together top IT & OT security professionals from across Europe's biggest manufacturers – tasked with protecting us from the biggest cyber threats facing our manufacturers. Join the key security leaders from across Europe's biggest companies to network, learn, be inspired, and collaborate towards new strategies for cyber resilience.

Munich Messe, Germany; 27th – 28th February 2024

More details can be found on the following website:

https://europe.manusecevent.com/

ICS incidents

Hackers disrupt Beirut Airport

Hackers disrupted the operation of Beirut's international airport by manipulating flight information display screens to convey politically motivated messages, as reported by local media. The incident temporarily affected baggage inspection at Beirut-Rafic Al Hariri International Airport over the first weekend in January. The hackers replaced plane departure and arrival data with a statement accusing Hezbollah, an Iran-backed militant group based in Lebanon, of dragging the country into a conflict with Israel.

The message directed blame at Hezbollah, stating, "You bear your responsibility and its consequences, Hezbollah." While the attack briefly disrupted the passenger baggage inspection system, it did not impact the flight schedule, according to airport authorities. Additionally, hackers allegedly sent fake messages to some passengers on behalf of Middle East Airlines, a claim refuted by the airline.

Tensions between Lebanon and Israel have recently escalated, with frequent exchanges of fire between their forces. A reported Israeli strike in Lebanon resulted in the death of a senior commander in Hezbollah's elite forces. Israeli officials expressed a preference for restoring security without engaging in war with Hezbollah but emphasized readiness for such a scenario if necessary.

Two domestic hacker groups, The One Who Spoke and Soldiers of God, were implicated in the airport hack. Soldiers of God, known for campaigns against the LGBTQ+ community in Lebanon, denied involvement. Some sources, including a Lebanese TV channel and anonymous security insiders, suggested the possibility of external parties using the names of local hacker groups to cover their tracks or escalate tensions. The report indicated that local hackers might lack the necessary technologies for such an attack.

Lebanon's Minister of Public Works and Transportation, Ali Hamieh, disclosed during a press conference that approximately 70% of the hacked airport screens had resumed normal operation. To limit further damage, the airport was disconnected from the internet. The country's security services are actively investigating the incident, and Hamieh noted that a determination regarding the breach's origin (internal or external) would be made in the coming days.

The source is available on the following link:

https://therecord.media/beirut-airport-hack-information-screens-baggage-screening

Book recommendation

Industrial Security Operations Book Two (Security Officers Handbook)

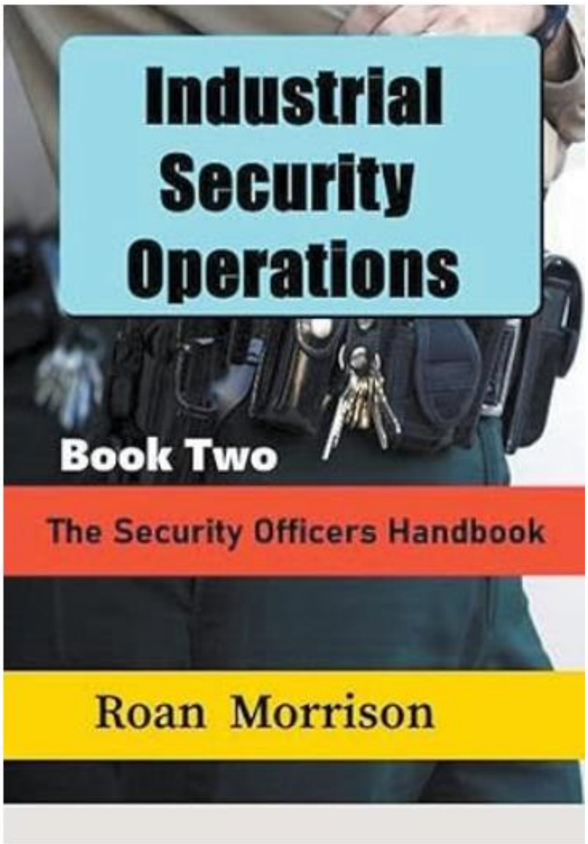
With ISO Book Two, you're no ordinary security officer! Become an elite senior security officer - with ISO Book Two, you'll gain the knowledge and skills you need to lead your team and serve as a trusted adviser to clients. Get up to speed on the latest international standards with this essential handbook - protect yourself and those around you with confidence!

Author/Editor: Roan Morrison

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/Industrial-Security-Operations-Officers-Handbook/dp/B0C58HRNHV#detailBullets_feature_div


Industrial Security Operations
Book Two
The Security Officers Handbook
Roan Morrison

ICS security news selection

States and Congress Wrestle With Cybersecurity After Iran Attacks Small Town Water Utilities

The hacking of a municipal water plant is prompting new warnings from U.S. security officials at a time when governments are wrestling with how to harden water utilities against cyberattacks.

The tiny Aliquippa water authority in western Pennsylvania was perhaps the least-suspecting victim of an international cyberattack.

It never had outside help in protecting its systems from a cyberattack, either at its existing plant that dates to the 1930s or the new $18.5 million one it is building.

Then it — along with several other water utilities — was struck by what federal authorities say are Iranian-backed hackers targeting a piece of equipment specifically because it was Israeli-made. …

Source and more information:

https://www.securityweek.com/states-and-congress-wrestle-with-cybersecurity-after-iran-attacks-small-town-water-utilities/

US, Israel Used Dutch Spy to Launch Stuxnet Malware Against Iran

Report tells US and Israel spent $1 billion to develop the infamous Stuxnet virus, built to sabotage Iran's nuclear program in 2008.

After a two-year investigation into the details surrounding the Stuxnet virus, unleashed in 2008 against the Iranian nuclear program, journalists with Dutch newspaper Volkskrant have released a report saying the malware cost $1 billion to develop.

Besides the enormous price tag, the outlet said a Dutch spy was used to release the Stuxnet virus into the Iranian nuclear infrastructure. The Dutch government told Volkskrant that the government understood the then-36-year-old Erik van Sabben was working to sabotage the Iranian nuclear project, however there was no knowledge of a cyber weapon of Stuxnet's consequence being used as part of the proceedings. …

Source and more information:

https://www.darkreading.com/ics-ot-security/us-israel-dutch-spy-stuxnet-malware-against-iran

CISA Urges Manufacturers to Eliminate Default Passwords After Recent ICS Attacks

The cybersecurity agency CISA is urging device manufacturers to stop relying on customers to change default passwords following a series of attacks targeting industrial control systems (ICS) in the water sector.

An alert released by CISA on Friday as part of its Secure by Design series recommends that manufacturers eliminate the risk associated with default passwords by implementing two principles: taking ownership of customer security outcomes, and building organizational structure and leadership to achieve such goals. …

Source and more information:

https://www.securityweek.com/cisa-urges-manufacturers-to-eliminate-default-passwords-after-recent-ics-attacks/

Industrial Defender collaborates with Dragos to enhance outcomes for OT operators

Industrial Defender announced a strategic technology partnership with Dragos.

The collaboration between these leaders in OT cybersecurity integrates their respective platform capabilities, representing a major move towards combining their leading strengths to enhance outcomes for OT operators.

The partnership is centered around the shared goal of enhancing the security and resilience of critical infrastructure and manufacturing facilities. The intent of this collaboration is to bring together the unique strengths of both Industrial Defender and Dragos. …

Source and more information:

https://www.helpnetsecurity.com/2024/01/17/industrial-defender-dragos-partnership/

New Findings Challenge Attribution in Denmark's Energy Sector Cyberattacks

The cyber attacks targeting the energy sector in Denmark last year may not have had the involvement of the Russia-linked Sandworm hacking group, new findings from Forescout show.

The intrusions, which targeted around 22 Danish energy organizations in May 2023, occurred in two distinct waves, one which exploited a security flaw in Zyxel firewall (CVE-2023-28771) and a follow-on activity cluster that saw the attackers deploy Mirai botnet variants on infected hosts via an as-yet-unknown initial access vector.

The first wave took place on May 11, while the second wave lasted from May 22 to 31, 2023. In one such attack detected on May 24, it was observed that the compromised system was communicating with IP addresses (217.57.80[.]18 and 70.62.153[.]174) that were previously used as command-and-control (C2) for the now-dismantled Cyclops Blink botnet. …

Source and more information:

https://thehackernews.com/2024/01/new-findings-challenge-attribution-in.html

ICS Ransomware Danger Rages Despite Fewer Attacks

Refined tactics, increased collaboration between groups, and continued success exploiting zero-days is helping ICS ransomware attackers inflict more damage, researchers find.

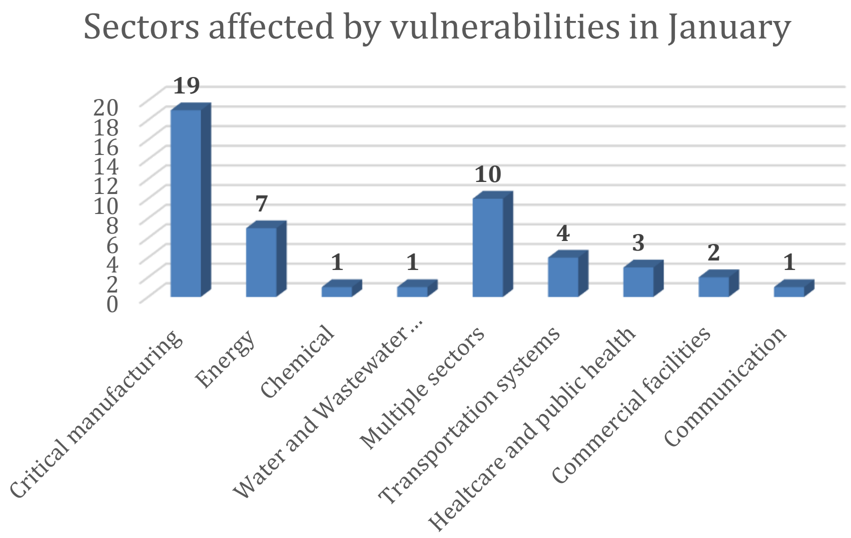
Despite takedowns of top ransomware groups, those remaining threat actors have continued to develop new tricks, while maintaining their ability to capitalize on zero-day vulnerabilities, helping them do more damage to industrial control systems (ICS) with fewer attacks, according to new research. …

Source and more information:

https://www.darkreading.com/ics-ot-security/ics-ransomware-rages-fewer-attacks

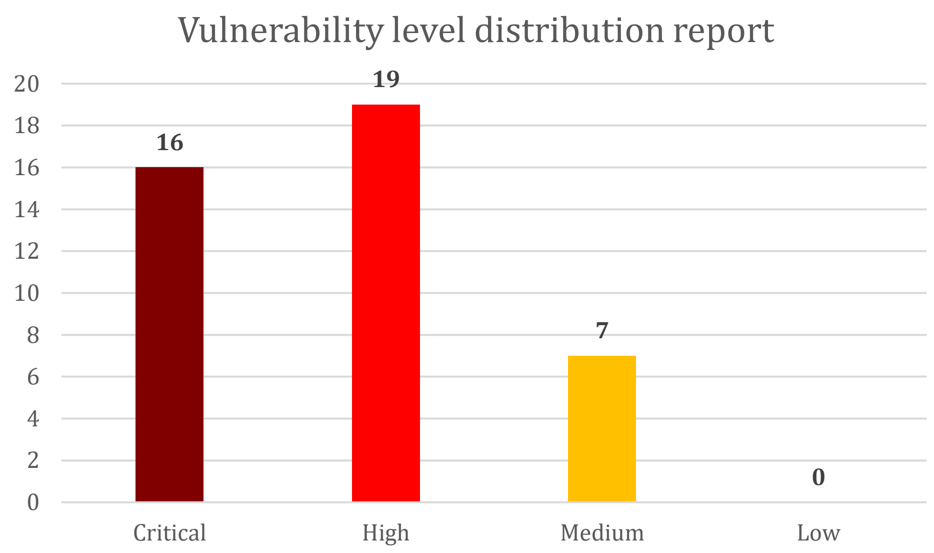
ICS vulnerabilities

In January 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 January:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	6
Cross-site Scripting	CWE-79	4
Missing Authentication for Critical Function	CWE-306	4
Stack-based Buffer Overflow	CWE-121	4



ICSA-24-030-01: **Emerson Rosemount GC370XA, GC700XA, GC1500XA**

Critical level vulnerabilities: Command Injection, Improper Authentication, Improper Authorization.

Emerson Rosemount GC370XA, GC700XA, GC1500XA | CISA

ICSA-24-030-02: **Mitsubishi Electric FA Engineering Software Products**

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

Mitsubishi Electric FA Engineering Software Products | CISA

ICSA-24-030-03: **Mitsubishi Electric MELSEC WS Series Ethernet Interface Module**

Medium level vulnerability: Authentication Bypass by Capture-replay.

Mitsubishi Electric MELSEC WS Series Ethernet Interface Module | CISA

ICSA-24-030-04: **Hitron Systems Security Camera DVR**

High level vulnerability: Improper Input Validation.

Hitron Systems Security Camera DVR | CISA

ICSA-24-030-05: **Rockwell Automation ControlLogix and GuardLogix**

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

Rockwell Automation ControlLogix and GuardLogix | CISA

ICSA-24-030-06: **Rockwell Automation FactoryTalk Service Platform**

Critical level vulnerability: Improper Verification of Cryptographic Signature.

Rockwell Automation FactoryTalk Service Platform | CISA

ICSA-24-030-07: **Rockwell Automation LP30/40/50 and BM40 Operator Interface**

High level vulnerabilities: Improper Validation of Consistency within Input, Out-of-bounds Write, Stack-based Buffer Overflow, Untrusted Pointer Dereference.

Rockwell Automation LP30/40/50 and BM40 Operator Interface | CISA

ICSA-23-208-03: **Mitsubishi Electric CNC Series (Update E)**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric CNC Series (Update E) | CISA

ICSA-24-025-01: **MachineSense FeverWarn**

Critical level vulnerabilities: Missing Authentication for Critical Function, Use of Hard-coded Credentials, Improper Access Control, OS Command Injection, Improper Restriction of Operations within the Bounds of a Memory Buffer.

MachineSense FeverWarn | CISA

ICSA-24-025-02: **SystemK NVR 504/508/516**

Critical level vulnerability: Command Injection.

SystemK NVR 504/508/516 | CISA

ICSA-24-023-01: **APsystems Energy Communication Unit (ECU-C) Power Control Software**

High level vulnerability: Improper Access Control.

APsystems Energy Communication Unit (ECU-C) Power Control Software | CISA

ICSA-24-023-02: **Crestron AM-300**

High level vulnerability: OS Command Injection.

Crestron AM-300 | CISA

ICSA-24-023-03: **Voltronic Power ViewPower Pro**

Critical level vulnerabilities: Deserialization of Untrusted Data, Missing Authentication for Critical Function, Exposed Dangerous Method or Function, OS Command Injection.

Voltronic Power ViewPower Pro | CISA

ICSA-23-023-04: **Westermo Lynx 206-F2G**

High level vulnerabilities: Cross-site Scripting, Code Injection, Cross-Origin Resource Sharing, Cleartext Transmission of Sensitive Information, Cross-Site Request Forgery.

Westermo Lynx 206-F2G | CISA

ICSA-24-023-05: **Lantronix XPort**

Medium level vulnerability: Weak Encoding for Password.

Lantronix XPort | CISA

ICSMA-24-023-01: **Orthanc Osimis DICOM Web Viewer**

High level vulnerability: Cross-site Scripting.

Orthanc Osimis DICOM Web Viewer | CISA

ICSA-24-018-01: **AVEVA PI Server**

High level vulnerabilities: Improper Check or Handling of Exceptional Conditions, Missing Release of Resource after Effective Lifetime.

AVEVA PI Server | CISA

ICSA-24-016-01: **SEW-EURODRIVE MOVITOOLS MotionStudio**

Medium level vulnerability: Improper Restriction of XML EXTERNAL Entity Reference.

SEW-EURODRIVE MOVITOOLS MotionStudio | CISA

ICSA-24-016-02: **Integration Objects OPC UA Server Toolkit**

Medium level vulnerability: Improper Output Neutralization for Logs.

Integration Objects OPC UA Server Toolkit | 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: 1.1)**

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: **Web Interface of 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: **GNU/Linux subsystem of the Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1** **(Update: 1.1)**

Critical level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

ICSA-24-011-03: **Rapid Software LLC Rapid SCADA**

Critical level vulnerabilities: Path Traversal, Relative Path Traversal, Local Privilege Escalation through Incorrect Permission Assignment for Critical Resource, Open Redirect, Use of Hard-coded Credentials, Plaintext Storage of a Password, Generation of Error Message Containing Sensitive Information.

Rapid Software LLC Rapid SCADA | CISA

ICSA-24-011-04: **Horner Automation Cscape**

High level vulnerability: Stack-Based Buffer Overflow.

Horner Automation Cscape | CISA

ICSA-24-011-05: **Schneider Electric Easergy Studio**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric Easergy Studio | CISA

ICSA-24-011-06: **Siemens Teamcenter Visualization and JT2Go**

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

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-011-07: **Siemens Spectrum Power 7**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens Spectrum Power 7 | CISA

ICSA-24-011-08: **Siemens SICAM A8000**

Medium level vulnerability: Use of Uninitialized Resource.

Siemens SICAM A8000 | CISA

ICSA-24-011-09: **Siemens SIMATIC CN 4100**

Critical level vulnerabilities: Authorization Bypass Through User-Controlled Key, Improper Input Validation, Use of Default Credentials.

Siemens SIMATIC CN 4100 | CISA

ICSA-24-011-10: **Siemens SIMATIC**

Critical level vulnerability: Improper Input Validation.

Siemens SIMATIC | CISA

ICSA-24-011-11: **Siemens Solid Edge**

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

Siemens Solid Edge | CISA

ICSA-23-348-01: **Cambium ePMP 5GHz Force 300-25 Radio (Update A)**

High level vulnerability: Code Injection.

Cambium ePMP 5GHz Force 300-25 Radio (Update A) | CISA

ICSA-24-004-01: **Rockwell Automation FactoryTalk Activation**

Critical level vulnerability: Out-of-Bounds Write.

Rockwell Automation FactoryTalk Activation | CISA

ICSA-24-004-02: **Mitsubishi Electric Factory Automation Products**

High level vulnerabilities: Observable Timing Discrepancy, Double Free, Access of Resource Using Incompatible Type ('Type Confusion').

Mitsubishi Electric Factory Automation Products | CISA

ICSA-23-348-15: **Unitronics Vision and Samba Series (Update A)**

Critical level vulnerability: Initialization of a Resource with an Insecure Default.

Unitronics Vision and Samba Series (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 January:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-7024 Google Chromium WebRTC Heap Buffer Overflow Vulnerability;
CVE-2023-7101 Spreadsheet::ParseExcel Remote Code Execution Vulnerability;
CVE-2023-38203 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability;
CVE-2023-29300 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability;
CVE-2023-27524 Apache Superset Insecure Default Initialization of Resource Vulnerability;
CVE-2023-41990 Apple Multiple Products Code Execution Vulnerability;
CVE-2016-20017 D-Link DSL-2750B Devices Command Injection Vulnerability;
CVE-2023-23752 Joomla! Improper Access Control Vulnerability;
CVE-2023-29357 Microsoft SharePoint Server Privilege Escalation Vulnerability;
CVE-2024-21887 Ivanti Connect Secure and Policy Secure Command Injection Vulnerability;
CVE-2023-46805 Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability;
CVE-2018-15133 Laravel Deserialization of Untrusted Data Vulnerability;
CVE-2023-6549 Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability;
CVE-2023-6548 Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability;
CVE-2024-0519 Google Chromium V8 Out-of-Bounds Memory Access Vulnerability;
CVE-2023-35082 Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability;
CVE-2023-34048 VMware vCenter Server Out-of-Bounds Write Vulnerability;
CVE-2024-23222 Apple Multiple Products Type Confusion Vulnerability;
CVE-2023-22527 Atlassian Confluence Data Center and Server Template Injection Vulnerability;
CVE-2022-48618 Apple Multiple Products Improper Authentication Vulnerability;
CVE-2024-21893 Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability;
Links and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two 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 One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

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

Fortinet Releases Security Updates for FortiOS and FortiProxy
Fortinet has released a security update to address a vulnerability in FortiOS and FortiProxy software. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Fortinet Releases Security Updates for FortiOS and FortiProxy | 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

Ivanti Releases Security Update for Connect Secure and Policy Secure Gateways
Ivanti has released a security update to address an authentication bypass vulnerability (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887) in all supported versions (9.x and 22.x) of Connect Secure and Policy Secure gateways. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.
Links and more information:
Ivanti Releases Security Update for Connect Secure and Policy Secure Gateways | CISA

Cisco Releases Security Advisory for Cisco Unity Connection
Cisco released a security advisory to address a vulnerability (CVE-2024-20272) in Cisco Unity Connection. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Cisco Releases Security Advisory for Cisco Unity Connection | CISA

Juniper Networks Releases Security Bulletin for Junos OS and Junos OS Evolved
Juniper Networks has released a security advisory to address a vulnerability (CVE-2024-21611) in Junos OS and Junos OS Evolved. 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 and Junos OS Evolved | CISA]

CISA and FBI Release Known IOCs Associated with Androxgh0st Malware
CISA and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Advisory (CSA), Known Indicators of Compromise Associated with Androxgh0st Malware, to disseminate known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with threat actors deploying Androxgh0st malware.
Links and more information:
[CISA and FBI Release Known IOCs Associated with Androxgh0st Malware | CISA]

VMware Releases Security Advisory for Aria Operations
VMware released a security advisory to address a vulnerability (CVE-2023-34063) in Aria Operations. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
[VMware Releases Security Advisory for Aria Operations | CISA]

Atlassian Releases Security Updates for Multiple Products
Atlassian released a security advisory to address a vulnerability (CVE-2023-22527) in out-of-date versions of Confluence Data Center and Server as well as its January 2024 security bulletin to address vulnerabilities in multiple products. A malicious cyber actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
[Atlassian Releases Security Updates for Multiple Products | CISA]

Citrix Releases Security Updates for NetScaler ADC and NetScaler Gateway
Citrix released security updates to address vulnerabilities (CVE-2023-6548 and CVE-2023-6549) in NetScaler ADC and NetScaler Gateway. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
[Citrix Releases Security Updates for NetScaler ADC and NetScaler Gateway | CISA]

Oracle Releases Critical Patch Update Advisory for January 2024
Oracle released its Critical Patch Update Advisory for January 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 January 2024 | CISA]

Drupal Releases Security Advisory for Drupal Core

Drupal released a security advisory to address a vulnerability affecting multiple Drupal core versions. A cyber threat actor could exploit this vulnerability to cause a denial-of-service condition.

Links and more information:
Drupal Releases Security Advisory for Drupal Core | CISA

Incident Response Guide for the WWS Sector

CISA, the Federal Bureau of Investigation (FBI), and the Environmental Protection Agency released a joint Incident Response Guide for the Water and Wastewater Systems (WWS) Sector. The guide includes contributions from over 25 WWS Sector organizations spanning private industry, nonprofit, and government entities. This coordination enabled CISA, FBI, and EPA to develop a guide with meaningful value to WWS Sector organizations.

Links and more information:
Incident Response Guide for the WWS Sector | CISA

CISA Issues Emergency Directive on Ivanti Vulnerabilities

CISA has issued Emergency Directive (ED) 24-01 Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities in response to active vulnerabilities in the following Ivanti products: Ivanti Connect Secure and Ivanti Policy Secure.

Links and more information:
CISA Issues Emergency Directive on Ivanti Vulnerabilities | CISA

Apple Releases Security Updates for Multiple Products

Apple has released security updates for iOS and iPadOS, macOS, Safari, watchOS, and tvOS. 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 Joins ACSC-led Guidance on How to Use AI Systems Securely

CISA has collaborated with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) on Engaging with Artificial Intelligence—joint guidance, led by ACSC, on how to use AI systems securely.

Links and more information:
CISA Joins ACSC-led Guidance on How to Use AI Systems Securely | CISA

Mozilla Releases Security Updates for Thunderbird and Firefox

Mozilla has released security updates to address vulnerabilities in Thunderbird and Firefox. 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 Thunderbird and Firefox | CISA]()

Cisco Releases Security Advisory for Multiple Unified Communications and Contact Center Solutions Products
Cisco released a security advisory to address a vulnerability (CVE-2024-20253) affecting multiple Unified Communications Products. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
[Cisco Releases Security Advisory for Multiple Unified Communications and Contact Center Solutions Products | CISA]()

Guidance: Assembling a Group of Products for SBOM
CISA published Guidance on Assembling a Group of Products created by the Software Bill of Materials (SBOM) Tooling & Implementation Working Group, one of the five SBOM community-driven workstreams facilitated by CISA.
Links and more information:
[Guidance: Assembling a Group of Products for SBOM | CISA]()

Juniper Networks Releases Security Bulletin for J-Web in Junos OS SRX Series and EX Series
Juniper Networks released a security bulletin to address multiple vulnerabilities for J-Web in Junos OS SRX Series and EX Series. 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 J-Web in Junos OS SRX Series and EX Series | CISA]()

New Mitigations to Defend Against Exploitation of Ivanti Connect Secure and Policy Secure Gateways
CISA is releasing this alert to provide cyber defenders with new mitigations to defend against threat actors exploiting Ivanti Connect Secure and Policy Secure Gateways vulnerabilities in Ivanti devices (CVE-2023-46805 and CVE-2024-21887).
Links and more information:
[New Mitigations to Defend Against Exploitation of Ivanti Connect Secure and Policy Secure Gateways | CISA]()

CISA and FBI Release Secure by Design Alert Urging Manufacturers to Eliminate Defects in SOHO Routers
CISA and the Federal Bureau of Investigation (FBI) published guidance on Security Design Improvements for SOHO Device Manufacturers as a part of the new Secure by Design (SbD) Alert series that focuses on how manufacturers should shift the burden of security away from customers by integrating security into product design and development.

Links and more information:
CISA and FBI Release Secure by Design Alert Urging Manufacturers to Eliminate Defects in SOHO Routers | CISA