2024 April, 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

- Q1: ICS Security In Review

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

Industrial Cybersecurity Pulse

- Ep. 44: Lesley Carhart on the regulations of AI in cybersecurity

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

Industrial Defender

Many podcasts available from 2023 on the following link in these themes:

- The Importance of OT Security,
- Bridging IT and OT,
- Best Practice & Compliance Frameworks,
- Vulnerabilities and Risk.

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

BEERISAC: OT/ICS Security Podcast Playlist

- Securing, Defending, and Bringing Resilience to Infrastructure (Hack the planet podcast)
- AI on the Menu: Cybersecurity Innovations with Dr. Ryan Heartfield in the Food Industry (Bites and bytes podcast)
- Energizing Cybersecurity Careers: Workforce Development in OT/ICS (Critical assets podcast)
- S2 E10 Meth and Giraffes (Working with lightning podcast)

- Claves para gestionar la ciberseguridad en la intersección de IT y OT (Secure tracks podcast)
- Addressing maritime cyber threats. (Control loop podcast)
- Udi Roth CISO @Mekorot Israel National Water Company on cyber defiance in critical OT infrastructure (ICS cyber talks)
- Ryan Pickren on New Web-Based PLC Malware Research (Aperture a Claroty podcast)
- Evaluating network segmentation strength (The Industrial Security Podcast)
- Welcome to PrOTect IT All (All things cybersecurity podcast from IT to OT)
- Dr Chuck Freilich Senior researcher @INSS on Iranian cyber threat & strategy effects on October 7th (ICS Cyber Talks podcast)
- OG of OT Official Teaser (The OG of OT podcast)
- Bridging the Gap: OT Cybersecurity in the Evolving Landscape of Industry and Recruitment (All things cybersecurity podcast from IT to OT)
- 3/4. Acciones en el Caso Realizando un test de intrusión en Sistemas de Control Industrial (Casos de Ciberseguridad Industrial podcast)
- WTF is OT? (The OG of OT)
- Exploring the OT Landscape: Insights from Building Management with Kyle Peters (All things cybersecurity podcast from IT to OT)
- From Segmentation to SOC: a Multilayered Approach to Cybersecurity in Rail Operations (Secure tracks podcast)
- Teaser #3 - The AI are Coming! (The OG of OT)
- Harnessing AI in Cybersecurity: Revolutionizing OT Protection (All things cybersecurity podcast from IT to OT)
- 4/4. Desenlace del Caso Realizando un test de intrusión en Sistemas de Control Industrial (Casos de Ciberseguridad Industrial)
- The Robot Rat Race (The OG of OT)
- Navigating Cybersecurity Challenges: A Conversation with Ted Gutierrez on Bridging OT and IT (All things cybersecurity podcast from IT to OT)
- 5 Ways to Make Your HMI Secure (Automation Chat)
- HMI S&M (The OG of OT)
- The Future of AI: Determinism, Security, and Beyond (All things cybersecurity podcast from IT to OT)
- Moty Cristal CEO @NEST on ransomware negotiation with hackers/attack groups: flipping the other side (ICS Cyber Talks podcast)
- Securing OT: Strategies for Prioritizing Vulnerabilities (All things cybersecurity podcast from IT to OT)

- Multiple Choice (The OG of OT)
- Tipisodes: 7 Steps To Better Cybersecurity (Process Safety podcast)
- Navigating China's infrastructure risks in the energy sector. (Control Loop: The OT Cybersecurity podcast)
- OT Security Made Simple | Wie entwickelt sich der OT-Markt (aus Investorensicht)? (OT Security Made Simple podcast)
- Alliance in Action: Industry Collaboration for Safer Food and Agriculture with Scott Algeier (Bites & Bytes podcast)
- 1/4. Contexto del Caso La importancia del contexto en la Ciberseguridad Industrial (Casos de Ciberseguridad Industrial podcast)
- 2/4. Análisis del Caso La importancia del contexto en la Ciberseguridad Industrial (Casos de Ciberseguridad Industrial)
- NCF-347 Cyber Physical Security (New Cyber Frontier podcast)
- teissTalk: Assessing and mitigating risks in your OT environment (teissPodcast - Cracking Cyber Security)
- Hunting for "Living off the Land" Activity (The Defender's Advantage podcast)
- 3/4. Acciones del Caso La importancia del contexto en la Ciberseguridad Industrial (Casos de Ciberseguridad Industrial podcast)
- Greg Garcia on the Change Healthcare Cyberattack (Aperture a Claroty podcast)
- Modern industrial control system security issues | Guest Thomas Pace (Cyber Work podcast)
- Hunting adversaries. (Control Loop: The OT Cybersecurity podcast)
- Inside (The OG of OT podcast)

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

ICS good practices, recommendations

IT Vs. OT Security

Geekflare published an article, Operational Technology (OT) Security Best Practices in 2024, which contains a number of useful facts about OT security. We would like to draw your attention to a comparison between IT and OT security, which can help you understand what you need to pay attention to in one area or the other. Without this understanding, it is impossible to work in harmony between the two areas.

Features	IT Security	OT Security
Deployment	At workplaces, on websites, in apps, etc.	Deployed in manufacturing plants, utility control facilities, airport baggage handling, waste management plants, etc.
Technology used	Always use state-of-the-art security encryption and protocols	Mostly use outdated technology since these are less exposed
Exposure	Always exposed to the public internet	OT security handles intranet cyber threats and is often not exposed to the public internet
Security tools	Antivirus, security patches, encryption, authentication, captcha, OTP, 2FA, etc.	Hardware security like IIOT protection shields, network switches with firewalls, biometric scanners, security cameras with OCR and face recognition, motion sensor, fire alarm, fire extinguisher, etc.
Target	IT security protects data, credentials, identity, assets, money, etc.	OT security protects industry machinery, access doors, inventory, command codes, manufacturing processes, etc.

We recommend reading the full article to consider the recommendations relevant to OT security.

Source, and more information available on the following link:

https://geekflare.com/operational-technology-security-best-practices/

ICS trainings, education

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

NEW! in this feed:

- OT/IT Security Training

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

ICS conferences

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

OT/ICS Virtual Cybersecurity Summit

Come and join forces with fellow OT/ICS (Operational Technology/Industrial Control Systems) cybersecurity professionals at the OT/ICS Cybersecurity Virtual Summit, where you'll gain vital insights to adeptly navigate the intricate landscape of cyber threats in 2024. Immerse yourself in the wisdom shared by industry experts and influential leaders, while also engaging directly with representatives from top-tier global providers of cybersecurity solutions tailored for the OT/ICS domain.

Virtual; 2nd May 2024

More details can be found on the following website:

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

2024 Joint NDIA/AIA Spring Industrial Security Conference

This bi-annual conference, presented in partnership with the Aerospace Industries Association (AIA), serves as the forum for executive-level security leadership and policy-makers across the federal agencies and U.S. Industry to convene to address major government security topics. Don't miss this opportunity for candid discussion, high-level networking, and updates on important subjects.

Jacksonville, FL, USA; 5th – 8th May 2024

More details can be found on the following website:

https://www.ndia.org/events/2024/5/6/2024-spring-isc

RSA Conference 2024

RSA Conference 2024 Expo is where some of the industry's leading companies will present cutting-edge products and solutions that can help you secure your organization. Discuss your challenges, participate in hands-on demos, make new contacts, and get a sense of where the industry’s technology is going.

San Francisco, CA, USA; 6th – 9th May 2024

More details can be found on the following website:

https://www.industrialdefender.com/events/rsa-conference-2024

ICS incidents

Japanese optic manufacturer suffered an attack affected production

Hoya Corporation, a global leader in optical products manufacturing, disclosed that its operations have been impacted by a potential breach in its systems. The company, headquartered in Tokyo, revealed that certain production plants and the ordering system for select products have been affected by the incident.

The breach was first detected on March 30, originating from an IT system incident in one of its overseas offices. External forensic investigators were promptly engaged, revealing unauthorized access to the company's servers by a third party as the likely cause.

While inquiries have been made regarding the involvement of ransomware, Hoya has yet to provide confirmation. Notably, this isn't the first instance of cybersecurity concerns for Hoya, with previous reports of a ransomware attack in 2021 and a malware infection at a plant in 2019. In response to the breach, Hoya has taken steps to isolate the affected servers and has notified relevant authorities in the impacted countries. However, the exact locations of the affected facilities remain undisclosed.

With over 36,000 employees across 30 countries and regions, Hoya reported revenues of approximately $5.5 billion in 2023. Despite ongoing investigations, the full extent and repercussions of the breach are still being assessed. Efforts are underway to manage customer demand and minimize disruptions as much as possible.

The company is yet to ascertain if any confidential or personal data has been compromised. It also remains uncertain how this incident will impact Hoya's business performance, although the company has committed to promptly disclosing any such effects.

Hoya Corporation is renowned for its production of eyeglasses, contact lenses, medical endoscopes, and lenses for cataract surgery replacements.

This breach adds to a concerning trend of cybersecurity incidents affecting major Japanese corporations over the past year. Notable victims include Fujitsu, Japan Aviation Electronics, Seiko, Casio, YKK, and Eisai, underscoring the pervasive threat posed by cyber-attacks in today's digital landscape.

The source is available on the following link:

https://therecord.media/hoya-japan-cyberattack-affects-production

Book recommendation

Operational Technology: The Beginner's Guide

Are you interested in learning about Operational Technology (OT)? If so, then this book is for you! In this comprehensive guide, you'll learn everything you need to know about OT, from the basics to the most advanced concepts.

You'll learn about the critical aspects of OT, such as industrial control systems, network security, and cutting-edge security architectures. You'll also learn how to protect OT networks from cyber threats and how to leverage advanced security frameworks in OT.

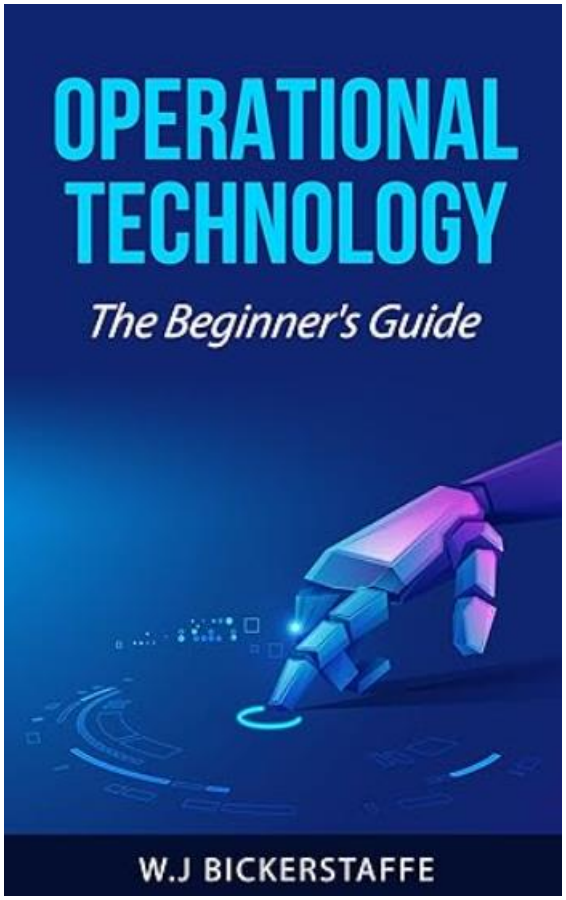
By the end of this book, you'll be an expert in Operational Technology. You'll be able to understand the critical aspects of OT, protect OT networks from cyber threats, and leverage advanced security frameworks in OT.

Author/Editor: William Bickerstaffe (Author)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/Operational-Technology-Beginners-Guide-Everything-ebook/dp/B0C98CP511



ICS security news selection

Industrial Cybersecurity Insights 2024

Operational technology (OT) is the umbrella term for the devices that control the physical processes of manufacturing and utility operations. It includes both industrial control systems and IIoT, and is foundational to manufacturing and critical industries.

OT differs in both evolution and purpose from information technology (IT). While IT is concerned with business data, OT is ultimately concerned with the physical processes of the shop floor (also known as cyber-physical). IT and OT are converging to allow business data influence over cyber-physical processes. This convergence is sometimes known as the Industry 4.0, and its purpose is to develop the smart factory. …

Source and more information:

https://www.securityweek.com/cyber-insights-2024-ot-ics-and-iiot/

Cyber attacks on critical infrastructure show advanced tactics and new capabilities

In this Help Net Security interview, Marty Edwards, Deputy CTO OT/IoT at Tenable, discusses the impact of geopolitical tensions on cyber attacks targeting critical infrastructure.

Edwards highlights the need for collaborative efforts between policymakers, government agencies, and the private sector to strengthen cybersecurity across critical infrastructure sectors. He emphasizes investment in personnel, technology, and proactive measures. …

Source and more information:

https://www.helpnetsecurity.com/2024/04/03/marty-edwards-tenable-critical-infrastructure-systems-cybersecurity/

Cyberattacks Wreaking Physical Disruption on the Rise

Ransomware groups tore into manufacturing other parts of the OT sector in 2023, and a few attacks caused eight- and nine-figure damages. But worse is yet to come in 2024. At least 68 cyberattacks last year caused physical consequences to operational technology (OT) networks at more than 500 sites worldwide — in some cases causing

$10 million to $100 million in damages. Unsurprisingly, these weren't Stuxnet-like events, but the opposite.

According to a new report from industrial control system (ICS) vendor Waterfall Security Solutions, which studied real-world cyberattacks on OT organizations, most of the hackers known to be targeting the OT sector these days are hacktivists. And the majority of disruptions are not caused by such direct manipulation of OT systems but are downstream consequences of IT-based attacks, most often involving ransomware. …

Source and more information:

https://www.darkreading.com/ics-ot-security/cyberattacks-wreaking-physical-disruption-on-the-rise

How can the energy sector bolster its resilience to ransomware attacks?

Since it plays a vital role in every functioning society, the energy sector has always been a prime target for state-backed cybercriminals. The cyber threats targeting this industry have grown significantly in recent years, as geopolitical tensions have fueled an increase in state-sponsored cyber espionage. According to one report on OT/ICS cyber security incidents, the energy sector recorded 39% of all attacks, with nearly 60% of these attacks attributed to state-affiliated groups. …

Source and more information:

https://www.helpnetsecurity.com/2024/04/08/energy-sector-attacks-resilience/

Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow

A hack that caused a small Texas town's water system to overflow in January has been linked to a shadowy Russian hacktivist group, the latest case of a U.S. public utility becoming a target of foreign cyberattacks.

The attack was one of three on small towns in the rural Texas Panhandle. Local officials said the public was not put in any danger and the attempts were reported to federal authorities. …

Source and more information:

https://www.securityweek.com/rural-texas-towns-report-cyberattacks-that-caused-one-water-system-to-overflow/

Geopolitical tensions escalate OT cyber attacks

In this Help Net Security interview, Andrew Ginter, VP of Industrial Security at Waterfall Security, discusses operational technology (OT) cyber attacks and their 2024 Threat Report. He examines how global geopolitical tensions and evolving ransomware tactics are reshaping industrial cybersecurity. He sheds light on the significance of recent incidents and the critical role of defensive strategies against these growing threats. …

Source and more information:

https://www.helpnetsecurity.com/2024/04/15/andrew-ginter-waterfall-security-ot-cyber-attacks/

ToddyCat APT Is Stealing Data on 'Industrial Scale'

An advanced persistent threat (APT) group known as ToddyCat is collecting data on an industrial scale from government and defense targets in the Asia-Pacific region.

Researchers from Kaspersky tracking the campaign described the threat actor this week as using multiple simultaneous connections into victim environments to maintain persistence and to steal data from them. They also discovered a set of new tools that ToddyCat (which is a common name for the Asian palm civet) is using to enable data collection from victim systems and browsers. …

Source and more information:

https://www.darkreading.com/cyber-risk/-toddycat-apt-is-stealing-data-on-an-industrial-scale-

DHS establishes AI Safety and Security Board to protect critical infrastructure

The Department of Homeland Security announced the establishment of the Artificial Intelligence Safety and Security Board (the Board). The Board will advise the Secretary, the critical infrastructure community, other private sector stakeholders, and the broader public on the safe and secure development and deployment of AI technology in nation's critical infrastructure.

The Board will develop recommendations to help critical infrastructure stakeholders, such as transportation service providers, pipeline and power grid operators, and internet service providers, more responsibly leverage AI technologies. It will also

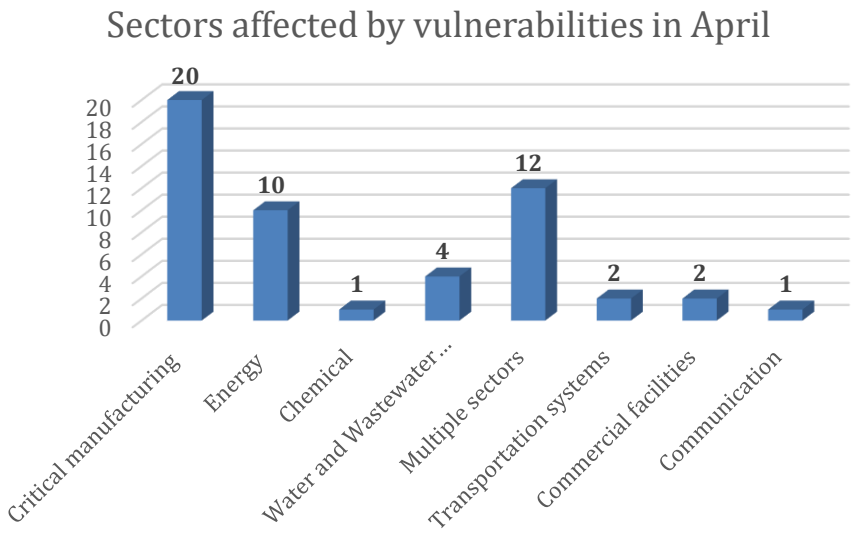
develop recommendations to prevent and prepare for AI-related disruptions to critical services that impact national or economic security, public health, or safety. …

Source and more information:

https://www.helpnetsecurity.com/2024/04/29/dhs-ai-safety-and-security-board/

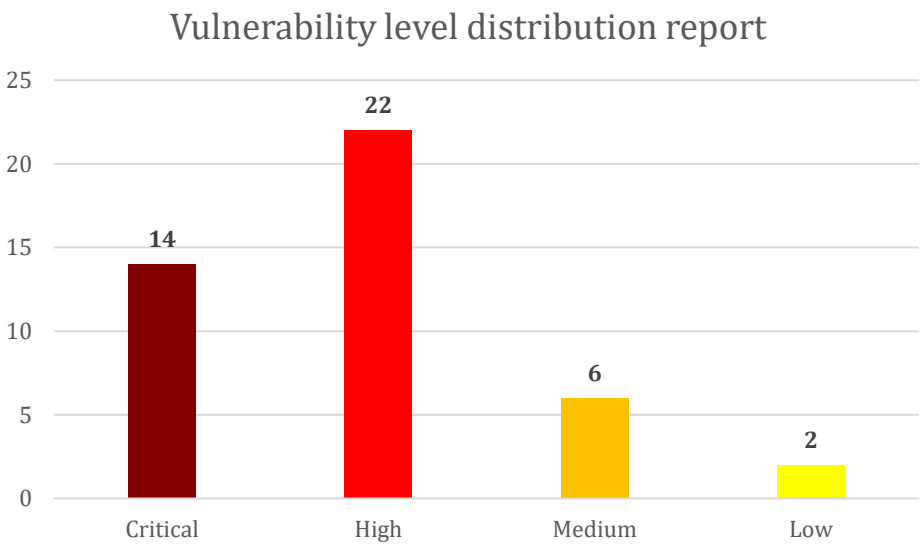
ICS vulnerabilities

In April 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 April:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	10
Classic Buffer Overflow	CWE.120	4
Improper Check for Unusual or Exceptional Conditions	CWE-754	4



ICSA-24-121-01: **Delta Electronics CNCSoft-G2 DOPSoft**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics CNCSoft-G2 DOPSoft | CISA

ICSA-24-016-01: **SEW-EURODRIVE MOVITOOLS MotionStudio (Update A)**

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

SEW-EURODRIVE MOVITOOLS MotionStudio (Update A) | CISA

ICSA-24-109-01: **Unitronics Vision Legacy Series (Update A)**

High level vulnerability: Storing Passwords in a Recoverable Format.

Unitronics Vision Legacy Series (Update A) | CISA

ICSA-24-116-01: **Multiple Vulnerabilities in Hitachi Energy RTU500 Series**

High level vulnerability: Unrestricted Upload of File with Dangerous Type.

Multiple Vulnerabilities in Hitachi Energy RTU500 Series | CISA

ICSA-24-116-02: **Hitachi Energy MACH SCM**

High level vulnerabilities: Improper Control of Generation of Code, Improper Neutralization of Directives in Dynamically Evaluated Code.

Hitachi Energy MACH SCM | CISA

ICSA-24-116-03: **Siemens RUGGEDCOM APE1808 Devices Configured with Palo Alto Networks Virtual NGFW**

Critical level vulnerability: Command Injection.

Siemens RUGGEDCOM APE1808 Devices Configured with Palo Alto Networks Virtual NGFW | CISA

ICSA-24-116-04: **Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager, Safety Manager SC**

Critical level vulnerabilities: Exposed Dangerous Method or Function, Absolute Path Traversal, Stack-based Buffer Overflow, Debug Messages Revealing Unnecessary Information, Out-of-bounds Write, Heap-based Buffer Overflow, Binding to an Unrestricted IP Address, Improper Input Validation, Buffer Access with Incorrect Length Value, Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Handling of Length Parameter Inconsistency.

Honeywell Experion PKS, Experion LX, PlantCruise by Experion, Safety Manager, Safety Manager SC | CISA

ICSA-23-143-03: **Mitsubishi Electric MELSEC Series CPU Module (Update D)**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric MELSEC Series CPU Module (Update D) | CISA

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

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

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

ICSA-24-102-09: **Rockwell Automation 5015-AENFTXT (Update A)**

High level vulnerability: Improper Input Validation.

Rockwell Automation 5015-AENFTXT (Update A) | CISA

ICSA-24-067-01: **Chirp Systems Chirp Access (Update B)**

Low level vulnerability: Use of Hard-coded Credentials.

Chirp Systems Chirp Access (Update B) | CISA

ICSA-24-051-03: **Mitsubishi Electric Electrical Discharge Machines (Update A)**

Critical level vulnerability: Improper Input Validation.

Mitsubishi Electric Electrical Discharge Machines (Update A) | CISA

ICSA-24-067-01: **Chirp Systems Chirp Access (Update A)**

Critical level vulnerability: Use of Hard-coded Credentials.

Chirp Systems Chirp Access (Update A) | CISA

SSA-832273: **Siemens RUGGEDCOM APE1808 devices (Update 1.1)**

Critical level vulnerabilities: Heap-based Buffer Overflow, External Control of File Name or Path, Out-of-bounds Write, Stack-based Buffer Overflow, Improper Privilege Management, Uncontrolled Resource Consumption, Improper Authentication, Improper Certificate Validation, Authorization Bypass Through User-Controlled Key, Use of Externally-Controlled Format String.

SSA-832273 (siemens.com)

SSA-831302: **Siemens SIMATIC S7-1500 TM MFP before V1.3.0 (Update 1.4)**

Critical level vulnerabilities: Multiple.

SSA-831302 (siemens.com)

SSA-794697: **Siemens SIMATIC S7-1500 TM MFP before V1.1 (Update 1.8)**

Critical level vulnerabilities: Multiple.

SSA-794697 (siemens.com)

SSA-753746: **Siemens SIMATIC WinCC Affecting Other SIMATIC Software Products (Update 1.1)**

High level vulnerability: NULL Pointer Dereference.

SSA-753746 (siemens.com)

SSA-716164: **Siemens Scalance W1750D (Update 1.1)**

Critical level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Input Validation, Improper Neutralization of Special Elements used in a Command ('Command Injection').

SSA-716164 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update 2.6)**

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

SSA-712929 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update 1.7)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-691715: **Siemens Products (Update 1.4)**

High level vulnerability: Improper Input Validation.

SSA-691715 (siemens.com)

SSA-457702: **Siemens SCALANCE W700 Product Family (Update 1.1)**

High level vulnerability: Authentication Bypass by Spoofing.

SSA-457702 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU (Update 1.4)**

Critical level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-203374: **Siemens SCALANCE W1750D Devices (Update 1.2)**

High level vulnerabilities: Inadequate Encryption Strength, Double Free, Use After Free, Improper Input Validation.

SSA-203374 (siemens.com)

ICSA-24-109-01: **Unitronics Vision Series PLCs**

High level vulnerability: Storing Passwords in a Recoverable Format.

Unitronics Vision Series PLCs | CISA

ICSA-21-287-03: **Mitsubishi Electric MELSEC iQ-R Series (Update B)**

Critical level vulnerability: Cleartext Transmission of Sensitive Information.

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

ICSA-21-250-01: **Mitsubishi Electric MELSEC iQ-R Series (Update B)**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Insufficiently Protected Credentials, Overly Restrictive Account Lockout Mechanism.

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

ICSA-24-107-01: **Measuresoft ScadaPro**

Medium level vulnerability: Improper Access Control.

Measuresoft ScadaPro | CISA

ICSA-24-107-02: **Electrolink FM/DAB/TV Transmitter**

High level vulnerabilities: Authentication Bypass by Assumed-Immutable Data, Reliance on Cookies without Validation and Integrity Checking, Missing Authentication for Critical Function, Cleartext Storage of Sensitive Information.

Electrolink FM/DAB/TV Transmitter | CISA

ICSA-24-107-03: **Rockwell Automation ControlLogix and GuardLogix**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix and GuardLogix | CISA

ICSA-24-107-04: **RoboDK RoboDK**

Low level vulnerability: Heap-based Buffer Overflow.

RoboDK RoboDK | CISA

ICSA-24-102-01: **Siemens SIMATIC S7-1500**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Improper Input Validation, Use After Free, Out-of-bounds Write.

Siemens SIMATIC S7-1500 | CISA

ICSA-24-102-02: **Siemens SIMATIC WinCC**

Medium level vulnerability: Classic Buffer Overflow.

Siemens SIMATIC WinCC | CISA

ICSA-24-102-03: **Siemens RUGGEDCOM APE1808 before V11.0.1**

Medium level vulnerabilities: Network Amplification, Exposure of Sensitive System Information to an Unauthorized Control Sphere, External Control of File Name or Path, Cross-site Scripting, Insufficiently Protected Credentials, Externally Controlled Reference to a Resource in Another Sphere.

Siemens RUGGEDCOM APE1808 before V11.0.1 | CISA

ICSA-24-102-04: **Siemens RUGGEDCOM APE1808**

High level vulnerabilities: Cross-site Scripting, Improper Privilege Management, Improper Check for Unusual or Exceptional Conditions, Truncation of Security-relevant Information, Insufficient Session Expiration.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-102-05: **Siemens Scalance W1750D**

Critical level vulnerability: Classic Buffer Overflow.

Siemens Scalance W1750D | CISA

ICSA-24-102-06: **Siemens Parasolid**

High level vulnerabilities: Out-of-bounds Read, Allocation of Resources Without Limits or Throttling, NULL Pointer Dereference.

Siemens Parasolid | CISA

ICSA-24-102-07: **Siemens SINEC NMS**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Improper Limitation of a Pathname to a Restricted Directory.

Siemens SINEC NMS | CISA

ICSA-24-102-08: **Siemens Telecontrol Server Basic**

High level vulnerabilities: Inadequate Encryption Strength, Double Free, Integer Overflow or Wraparound, External Control of File Name or Path, Path Traversal, Improper Input Validation, Missing Encryption of Sensitive Data, Use After Free, Improper Certificate Validation, Inefficient Regular Expression Complexity, Improper Check for Unusual or Exceptional Conditions, NULL Pointer Dereference, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Telecontrol Server Basic | CISA

ICSA-24-102-09: **Rockwell Automation 5015-AENFTXT**

High level vulnerability: Improper Input Validation.

Rockwell Automation 5015-AENFTXT | CISA

ICSA-24-100-01: **SUBNET PowerSYSTEM Server and Substation Server**

High level vulnerability: Reliance on Insufficiently Trustworthy Component.

SUBNET PowerSYSTEM Server and Substation Server | CISA

ICSA-24-095-01: **Hitachi Energy Asset Suite 9**

Medium level vulnerability: Improper Authentication.

Hitachi Energy Asset Suite 9 | CISA

ICSA-24-095-02: **Schweitzer Engineering Laboratories SEL**

Medium level vulnerability: Inclusion of Undocumented Features.

Schweitzer Engineering Laboratories SEL | CISA

ICSA-24-093-01: **IOSIX IO-1020 Micro ELD**

Critical level vulnerabilities: Use of Default Credentials, Download of Code Without Integrity Check.

IOSIX IO-1020 Micro ELD | 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 April:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-29745 Android Pixel Information Disclosure Vulnerability;
CVE-2024-29748 Android Pixel Privilege Escalation Vulnerability;
CVE-2024-3272 D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability;
CVE-2024-3273 D-Link Multiple NAS Devices Command Injection Vulnerability;
CVE-2024-3400 Palo Alto Networks PAN-OS Command Injection Vulnerability;
CVE-2022-38028 Microsoft Windows Print Spooler Privilege Escalation Vulnerability;
CVE-2024-20353 Cisco ASA and FTD Denial of Service Vulnerability;
CVE-2024-20359 Cisco ASA and FTD Privilege Escalation Vulnerability;
CVE-2024-4040 CrushFTP VFS Sandbox Escape Vulnerability;
CVE-2024-29988 Microsoft SmartScreen Prompt Security Feature Bypass Vulnerability;
Links and more information:
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
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 Publishes New Webpage Dedicated to Providing Resources for High-Risk Communities
CISA published a new dedicated High-Risk Communities webpage comprised of cybersecurity resources to support civil society communities at heighted risk of digital security threats, including cyber hygiene guidance, a repository of local cyber volunteer programs, and free or discounted tools and services.
Links and more information:
CISA Publishes New Webpage Dedicated to Providing Resources for High-Risk Communities | CISA

Ivanti Releases Security Update for Ivanti Connect Secure and Policy Secure Gateways
Ivanti has released security updates to address vulnerabilities in all supported versions (9.x and 22.x) of Ivanti Connect Secure and Policy Secure gateways. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
Ivanti Releases Security Update for Ivanti Connect Secure and Policy Secure Gateways | CISA

Fortinet Releases Security Updates for Multiple Products
Fortinet released security updates to address vulnerabilities in multiple products, including OS and FortiProxy. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Fortinet Releases Security Updates for Multiple Products | CISA

Microsoft Releases April 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 April 2024 Security Updates | CISA

Adobe Releases Security Updates for Multiple Products
Adobe has 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 Issues Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System
CISA publicly issued Emergency Directive (ED) 24-02 to address the recent campaign by Russian state-sponsored cyber actor Midnight Blizzard to exfiltrate email correspondence of Federal Civilian Executive Branch (FCEB) agencies through a successful compromise of Microsoft corporate email accounts.
Links and more information:
CISA Issues Emergency Directive 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System | CISA

Compromise of Sisense Customer Data
CISA is collaborating with private industry partners to respond to a recent compromise discovered by independent security researchers impacting Sisense, a company that provides data analytics services.
Links and more information:
Compromise of Sisense Customer Data | CISA

Juniper Releases Security Bulletin for Multiple Juniper Products
Juniper has released security updates to address multiple vulnerabilities in Junos OS, Junos OS Evolved, Paragon Active Assurance and Junos OS: EX4300 Series. A cyber threat actor could exploit some of these vulnerabilities to cause a denial-of-service condition.
Links and more information:

Juniper Releases Security Bulletin for Multiple Juniper Products | CISA

Citrix Releases Security Updates for XenServer and Citrix Hypervisor

Citrix released security updates to address multiple vulnerabilities in XenServer and Citrix Hypervisor. 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 XenServer and Citrix Hypervisor | CISA

Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400

Palo Alto Networks has released workaround guidance for a command injection vulnerability (CVE-2024-3400) affecting PAN-OS versions 10.2, 11.0, and 11.1. Palo Alto Networks has reported active exploitation of this vulnerability in the wild.

Links and more information:

Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400 | CISA

Joint Guidance on Deploying AI Systems Securely

National Security Agency's Artificial Intelligence Security Center (NSA AISC) published the joint Cybersecurity Information Sheet Deploying AI Systems Securely in collaboration with CISA, the Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ASD ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK).

Links and more information:

Joint Guidance on Deploying AI Systems Securely | CISA

Oracle Releases Critical Patch Update Advisory for April 2024

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

CISA and Partners Release Advisory on Akira Ransomware

CISA, the Federal Bureau of Investigation (FBI), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Akira Ransomware, to disseminate known Akira ransomware tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as February 2024.

Links and more information:

CISA and Partners Release Advisory on Akira Ransomware | CISA

Cisco Releases Security Advisories for Cisco Integrated Management Controller

Cisco has released security advisories for vulnerabilities in the Cisco integrated management controller. A remote cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Cisco Releases Security Advisories for Cisco Integrated Management Controller | CISA

Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms

Cisco released security updates to address ArcaneDoor—exploitation of Cisco Adaptive Security Appliances (ASA) devices and Cisco Firepower Threat Defense (FTD) software. A cyber threat actor could exploit vulnerabilities (CVE-2024-20353, CVE-2024-20359, CVE-2024-20358) to take control of an affected system.

Links and more information:

Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms | CISA