2023 July, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, 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 good practices, recommendations

ENISA Threat Landscape Health sector

The first ENISA health landscape includes reported cyber incidents affecting various types of organisations related to health such as:

- healthcare providers, such as hospitals, primary care providers, sociosanitary care providers, dental care providers, emergency services, mental health institutions, etc.,
- EU reference laboratories, entities carrying out research and development activities for medicinal products and, more generally, organisations conducting health related research,
- entities manufacturing basic pharmaceutical products and pharmaceutical preparations, and the pharmaceutical industry in general,
- entities manufacturing medical devices and biotechnology manufacturers,
- health authorities, bodies and agencies nationally and in the EU,
- health insurance organisations,
- residential treatment facilities and social services providers.

To conduct this study, the ENISA Cybersecurity Threat Landscape Methodology was applied. Data collection and analysis focused on cyber incidents observed in EU member states and neighbouring countries (Norway, Switzerland and the United Kingdom). This is by no means the complete list of incidents that occurred during the reporting period.

ENISA gathered a list of major incidents based on open-source intelligence (OSINT) and ENISA's own cyber threat intelligence capabilities. The data collected were further analysed by ENISA's threat landscape team and external experts.

Source and more information available on the following link:

https://www.enisa.europa.eu/publications/health-threat-landscape

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in August 2023:

- 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/

- ICS/SCADA security training seminar

https://www.enoinstitute.com/scada-ics-security-training-seminar/

- 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 conferences

In August 2023, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Fortinet OT Industrial Security Days

Industries that rely industrial control systems (ICS) are looking to add new capabilities and improve operational efficiencies through the latest digital innovations. But as operational technology (OT) environments incorporate IT-based devices and applications, and integrate network connectivity, new pathways for cyber criminals arise exposing critical production systems to cyberattacks.

Today, there remains a high degree of variation in the OT security practices and capabilities used, including practices for securing legacy and modern equipment. To protect the critical infrastructure in OT, industrial organizations need to harness the power of a defense in depth strategy to secure their data, systems, and users, as well as minimize the risk of attackers gaining access to their critical infrastructure.

Buffalo, NY, USA; 8th August 2023

More details can be found on the following website:

https://industrialcyber.co/event/fortinet-ot-industrial-security-days-buffalo/

Fortinet OT Industrial Security Days

Industries that rely industrial control systems (ICS) are looking to add new capabilities and improve operational efficiencies through the latest digital innovations. But as operational technology (OT) environments incorporate IT-based devices and applications, and integrate network connectivity, new pathways for cyber criminals arise exposing critical production systems to cyberattacks.

Today, there remains a high degree of variation in the OT security practices and capabilities used, including practices for securing legacy and modern equipment. To protect the critical infrastructure in OT, industrial organizations need to harness the power of a defense in depth strategy to secure their data, systems, and users, as well as minimize the risk of attackers gaining access to their critical infrastructure.

St. Louis, MO, USA; 29th August 2023

More details can be found on the following website:

https://industrialcyber.co/event/fortinet-ot-industrial-security-days-stl/

ICS incidents

Japan’s largest port stops operations after ransomware attack

The Port of Nagoya, Japan's largest and busiest port, has experienced a ransomware attack that has severely impacted its container terminals. As a vital trade hub, the port handles approximately 10% of Japan's total trade volume, with millions of containers and cargo tonnage passing through it annually. The attack has disrupted the operation of the port's central control system, known as the Nagoya Port Unified Terminal System (NUTS), which manages all container terminals.

The ransomware attack was discovered on July 4, 2023, and has forced the port authority to cancel all container loading and unloading operations using trailers. The authorities have identified the cause of the problem as a ransomware infection and are working to restore the NUTS system by 6 PM. However, the financial losses and disruptions to the circulation of goods to and from Japan are expected to be significant.

Although the Port of Nagoya has dealt with previous cyberattacks, this ransomware incident has had the largest impact thus far. In September 2022, the port's website was targeted by a distributed denial-of-service (DDoS) attack, causing a temporary disruption. The identity of the threat actor responsible for the ransomware attack remains unknown, as no public claim of responsibility has been made at this time.

The incident highlights the vulnerability of critical infrastructure, such as major ports, to cyber threats. It underscores the need for robust cybersecurity measures and proactive defense strategies to protect essential systems and prevent disruptions that can have far-reaching economic consequences. Authorities are actively working to address the situation and restore normal operations as quickly as possible.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/japans-largest-port-stops-operations-after-ransomware-attack/

https://safety4sea.com/japans-nagoya-port-stops-container-operations-after-ransomware-attack/

Book recommendation

Operational Technology Security A Clear and Concise Reference

- Are you keeping current on recommended cybersecurity best practices?
- Do you have remote access to your ICS environment?
- Does the intelligence you action cover your most valuable information assets?
- How does the information flow through the system, and through what mechanisms?
- How to build a next generation mobile strategy?
- Is your ICS environment protected from the internet?
- What are the tools or perspectives necessary to do damage?
- What assets are you most concerned about from a cybersecurity perspective?
- Who can support you to manage and contain a security breach?
- Who is ultimately responsible for cybersecurity?

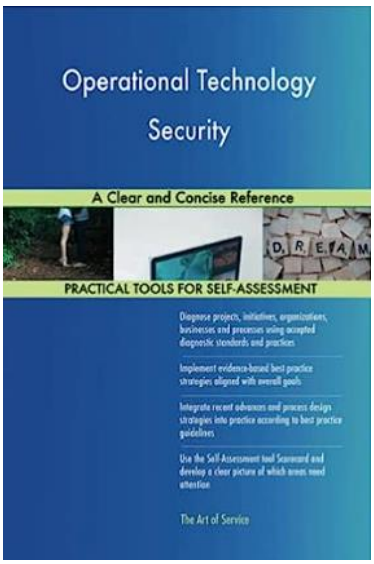
This Operational Technology Security Guide is unlike books you're used to. If you're looking for a textbook, this might not be for you. This book and its included digital components are for you who understands the importance of asking great questions. This gives you the questions to uncover the Operational Technology Security challenges you're facing and generate better solutions to solve those problems.

Authors/Editors: Gerardus Blokdyk (Author)

Year of issue: 2021

The book is available at the following link:

https://www.amazon.com/Operational-Technology-Security-Concise-Reference/dp/0655411941



ICS security news selection

Over 130,000 solar energy monitoring systems exposed online

Security researchers are warning that tens of thousands of photovoltaic (PV) monitoring and diagnostic systems are reachable over the public web, making them potential targets for hackers.

These systems are used for remote performance monitoring, troubleshooting, system optimization, and other functions to allow remote management of renewable energy production units.

Sensitive info exposed

Cyble's threat analysts scanned the web for internet-exposed PV utilities and found 134,634 products from various vendors, which include Solar-Log, Danfoss Solar Web Server, SolarView Contec, SMA Sunny Webbox, SMA Cluster Controller, SMA Power Reducer Box, Kaco New Energy & Web, Fronis Datamanager, Saj Solar Inverter, and ABB Solar Inverter Web GUI. …

Source, and more information:

https://www.bleepingcomputer.com/news/security/over-130-000-solar-energy-monitoring-systems-exposed-online/

Vulnerabilities in PiiGAB Product Could Expose Industrial Organizations to Attacks

Potentially serious vulnerabilities discovered by researchers in a PiiGAB product could expose industrial organizations to remote hacker attacks.

PiiGAB is a Sweden-based company that provides industrial and building automation hardware and software solutions.

Researchers Floris Hendriks and Jeroen Wijenbergh conducted an in-depth security assessment of PiiGAB's M-Bus 900s gateway/converter as part of their master's in cybersecurity at Radboud University in the Netherlands. The product is designed for the remote monitoring of devices using the M-Bus protocol. …

Source, and more information:

https://www.securityweek.com/vulnerabilities-in-piigab-product-could-expose-industrial-organizations-to-attacks/

How ransomware impacts the healthcare industry

Healthcare continues to be one of the most attractive targets for cyberattackers, and the number of breaches affecting the industry is increasing yearly.

In this Help Net Security video, Steve Gwizdala, VP of Healthcare at ForgeRock, discusses how vigilance and new ways of enhancing cybersecurity measures will be crucial to healthcare organizations and businesses responsible for protecting consumers' online information – across the entire supply chain.

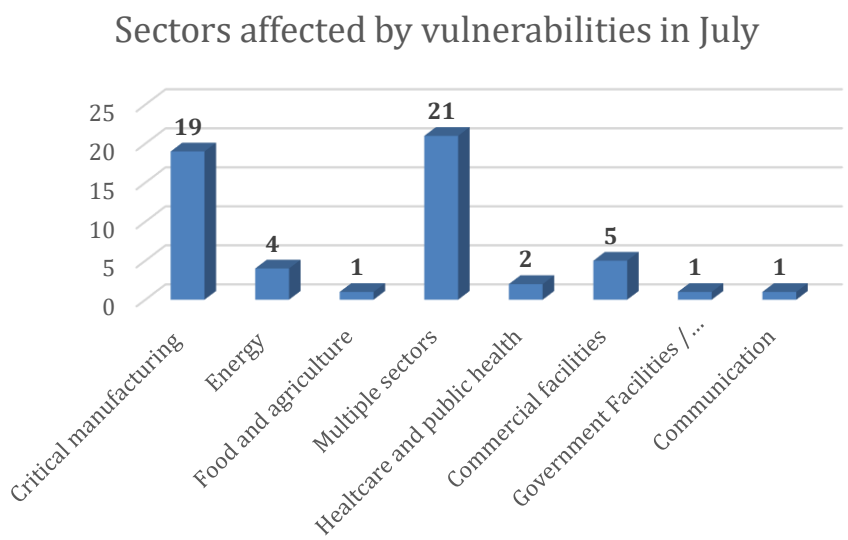
There needs to be more than the traditional password and username approach to protect such valuable information and keep healthcare organizations in business. …

Source, and more information:

https://www.helpnetsecurity.com/2023/07/05/how-ransomware-impacts-healthcare-industry-video/

ICS vulnerabilities

In July 2023, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

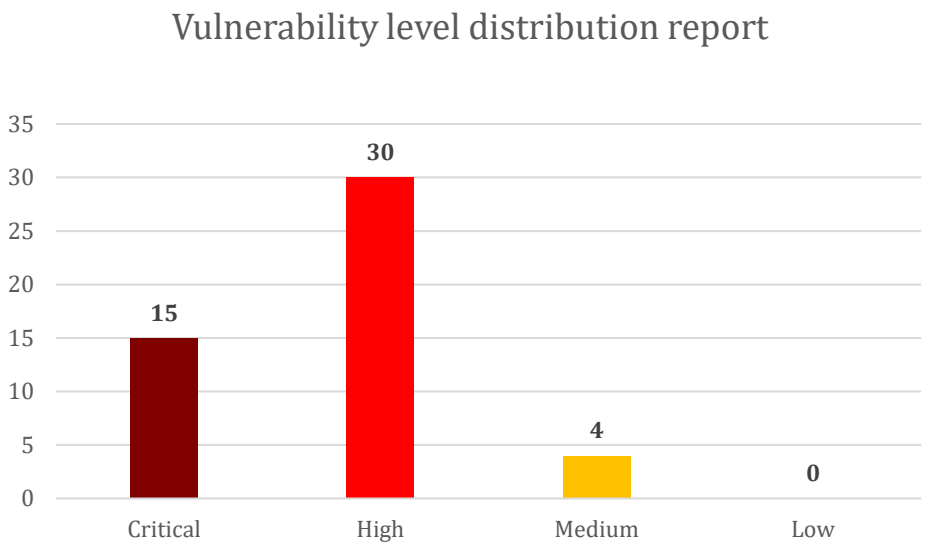


Average number of vulnerabilities per vulnerability report in July: **3,14**

Vulnerabilities/Exploitable remotely: **49/36**

The most common vulnerabilities in July:

Vulnerability	CWE number	Items
Uncontrolled Resource Consumption	CWE-400	8
Improper Input Validation	CWE-20	7
Classic Buffer Overflow	CWE.120	6
Improper Authentication	CWE-287	5



ICSA-23-208-01: **ETIC Telecom RAS Authentication**

High level vulnerability: Insecure Default Initialization of Resource.

ETIC Telecom RAS Authentication | CISA

ICSA-23-208-02: **PTC KEPServerEX**

High level vulnerability: Uncontrolled Resource Consumption.

PTC KEPServerEX | CISA

ICSA-23-208-03: **Mitsubishi Electric CNC Series**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric CNC Series | CISA

ICSA-22-307-01: **ETIC RAS (Update A)**

High level vulnerabilities: Insufficient Verification of Data Authenticity, Path Traversal, Unrestricted Upload of File with Dangerous Type.

ETIC Telecom Remote Access Server (RAS) (Update A) | CISA

ICSA-22-172-01: **Mitsubishi Electric MELSEC iQ-R, Q, L Series and MELIPC Series (Update B)**

High level vulnerability: Improper Resource Locking.

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

ICSA-23-206-01: **AXIS A1001**

High level vulnerability: Heap-based Buffer Overflow.

AXIS A1001 | CISA

ICSA-23-206-02: **Rockwell Automation ThinManager ThinServer**

High level vulnerability: Relative Path Traversal.

Rockwell Automation ThinManager ThinServer | CISA

ICSA-23-206-03: **Emerson ROC800 Series RTU and DL8000 Preset Controller**

Critical level vulnerability: Authentication Bypass.

Emerson ROC800 Series RTU and DL8000 Preset Controller | CISA

ICSA-23-206-04: **Johnson Controls IQ Wifi 6**

High level vulnerability: Improper Restriction of Excessive Authentication Attempts.

Johnson Controls IQ Wifi 6 | CISA

ICSA-23-201-01: **Schneider Electric EcoStruxure Products, Modicon PLCs, and Programmable Automation Controllers**

High level vulnerability: Improper Check for Unusual or Exceptional Conditions.

Schneider Electric EcoStruxure Products, Modicon PLCs, and Programmable Automation Controllers | CISA

ICSA-23-199-01: **Rockwell Automation Kinetix 5700 DC Bus Power Supply Series A** **High** level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation Kinetix 5700 DC Bus Power Supply | CISA

ICSA-23-199-02: **Keysight N6845A Geolocation Server**

High level vulnerabilities: Exposed Dangerous Method or Function, Relative Path Traversal.

Keysight N6845A Geolocation Server | CISA

ICSA-23-199-03: **Iagona ScrutisWeb**

Critical level vulnerabilities: Absolute Path Traversal, Authorization Bypass Through User-Controlled Key, Use of Hard-coded Cryptographic Key, Unrestricted Upload of File with Dangerous Type.

Iagona ScrutisWeb | CISA

ICSA-23-199-04: **Weintek Weincloud**

Critical level vulnerabilities: Weak Password Recovery Mechanism for Forgotten Password, Improper Authentication, Improper Restriction of Excessive Authentication Attempts, Improper Handling of Structural Elements.

Weintek Weincloud | CISA

ICSA-23-199-051: **GeoVision GV-ADR2701**

Critical level vulnerability: Improper Authentication.

GeoVision GV-ADR2701 | CISA

ICSA-23-199-06: **GE Cimplicity**

Medium level vulnerability: Heap-based Buffer Overflow.

GE Digital CIMPLICITY | CISA

ICSA-23-199-07: **WellinTech KingHistorian**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Signed to Unsigned Conversion Error.

WellinTech KingHistorian | CISA

SSA-968170: **SIMATIC STEP 7 V5.x and Derived Products (Update: 1.1)**

Critical level vulnerabilities: Improper Control of Generation of Code ('Code Injection').

SSA-968170 (siemens.com)

SSA-930100: **Simcenter STAR-CCM+ (Update: 1.1)**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

SSA-930100 (siemens.com)

SSA-794697: **SIMATIC S7-1500 TM MFP V1.0 (Update: 1.1)**

Critical level vulnerabilities: Multiple (33 vulnerabilities).

SSA-794697 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update: 2.2)**

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

SSA-712929 (siemens.com)

SSA-686975: **Siemens Industrial Products using Intel CPUs (Update: 1.2)**

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

SSA-686975 (siemens.com)

SSA-478960: **Web Server Login Page of Industrial Controllers (Update: 1.5)**

Medium level vulnerability: Cross-Site Request Forgery (CSRF).

SSA-478960 (siemens.com)

SSA-446448: **PROFINET Stack Integrated on Interniche Stack (Update: 1.9)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-446448 (siemens.com)

SSA-408105: **Siemens Products (Update: 1.2)**

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

SSA-408105 (siemens.com)

SSA-382653: Industrial Products **(Update: 1.4)**

High level vulnerabilities: Improper Input Validation, Improper Validation of Specified Quantity in Input, Improper Validation of Specified Type of Input, Improper Validation of Syntactic Correctness of Input.

SSA-382653 (siemens.com)

SSA-363107: SIMATIC WinCC Kiosk Mode **(Update: 1.2)**

High level vulnerability: Insecure Default Initialization of Resource.

SSA-363107 (siemens.com)

SSA-306654: Siemens Industrial Products **(Update: 1.6)**

High level vulnerabilities: Multiple (12 vulnerabilities)

SSA-306654 (siemens.com)

ICSA-23-194-01: **Siemens RUGGEDCOM ROX**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Command Injection, Improper Authentication, Classic Buffer Overflow, Uncontrolled Resource Consumption, Improper Certificate Validation, Cross-Site Request Forgery (CSRF), Improper Input Validation, Incorrect Default Permissions, Cross-site Scripting, Inadequate Encryption Strength, Use of a Broken or Risky Cryptographic Algorithm.

Siemens RUGGEDCOM ROX | CISA

ICSA-23-194-02: **Siemens SiPass Integrated**

High level vulnerability: Improper Input Validation.

Siemens SiPass Integrated | CISA

ICSA-23-194-04: **Siemens SIMATIC MV500 Devices**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Missing Release of Memory after Effective Lifetime, Injection, Inadequate Encryption Strength, Double Free, Incomplete Cleanup, Observable Discrepancy, Improper Locking, Use After Free, Improper Input Validation.

Siemens SIMATIC MV500 Devices | CISA

ICSA-23-194-05: **Rockwell Automation PowerMonitor 1000**

High level vulnerability: Cross-site Scripting.

Rockwell Automation PowerMonitor 1000 | CISA

ICSA-23-194-06: **Honeywell Experion PKS, LX and PlantCruise**

Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow, Out-of-bounds Write, Uncontrolled Resource Consumption, Improper Encoding or Escaping of Output, Deserialization of Untrusted Data, Improper Input Validation, Incorrect Comparison.

Honeywell Experion PKS, LX and PlantCruise | CISA

ICSMA-23-194-01: **BD Alaris System with Guardrails Suite MX**

High level vulnerabilities: Insufficient Verification of Data Authenticity, Missing Authentication for Critical Function, Improper Verification of Cryptographic Signature, Missing Support for Integrity Check, Cross-site Scripting, Cleartext Transmission of Sensitive Information, Improper Restriction of XML External Entity Reference.

BD Alaris System with Guardrails Suite MX | CISA

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

High level vulnerability: Improper Resource Shutdown or Release.

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

ICSA-23-171-01: **Enphase Envoy (Update A)**

Medium level vulnerability: OS Command Injection.

Enphase Envoy (Update A) | CISA

ICSA-23-193-01: **Rockwell Automation Select Communication Modules**

Critical level vulnerability: Out-of-bounds Write.

Rockwell Automation Select Communication Modules | CISA

ICSA-23-192-01: **Rockwell Automation Enhanced HIM**

Critical level vulnerability: Cross-site Request Forgery.

Rockwell Automation Enhanced HIM | CISA

ICSA-23-192-02: **Sensormatic Electronics iSTAR**

High level vulnerability: Improper Authentication.

Sensormatic Electronics iSTAR | CISA

ICSA-23-192-03: **Panasonic Control FPWin Pro7**

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

Panasonic Control FPWin Pro7 | CISA

ICSA-23-180-04: **Mitsubishi Electric MELSEC-F Series (Update A)**

High level vulnerability: Authentication Bypass by Capture-replay.

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

ICSA-23-187-01: **PiiGAB M-Bus**

Critical level vulnerabilities: Code Injection, Improper Restriction of Excessive Authentication Attempts, Unprotected Transport of Credentials, Use of Hard-coded Credentials, Plaintext Storage of a Password, Cross-site Scripting, Weak Password Requirements, Use of Password Hash with Insufficient Computational Effort, Cross-Site Request Forgery.

PiiGAB M-Bus | CISA

ICSA-23-187-02: **ABUS TVIP**

High level vulnerability: Command injection.

ABUS TVIP | CISA

ICSA-23-143-03: **Mitsubishi Electric MELSEC Series CPU module (Update A)**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric MELSEC Series CPU module (Update A) | CISA

ICSMA-23-180-01: **Medtronic Paceart Optima System**

Critical level vulnerability: Deserialization of Untrusted Data.

Medtronic Paceart Optima System | CISA

ICSA-19-120-01: **Rockwell Automation CompactLogix 5370 (Update A)**

High level vulnerabilities: Uncontrolled Resource Consumption, Stack-based Buffer Overflow.

Rockwell Automation CompactLogix 5370 (Update A) | CISA

ICSA-20-245-01: **Mitsubishi Electric Multiple Products (Update F)**

High level vulnerability: Predictable Exact Value from Previous Values.

Mitsubishi Electric Multiple Products (Update F) | CISA

ICSA-22-333-05: **Mitsubishi Electric FA Engineering Software (Update B)**

Critical level vulnerabilities: Cleartext Storage of Sensitive Information, Use of Hard-coded Password, Insufficiently Protected Credentials, Use of Hard-coded Cryptographic Key, Cleartext Storage of Sensitive Information in Memory.

Mitsubishi Electric FA Engineering Software (Update B) | CISA

ICSA-23-171-02: **Enphase Installer Toolkit Android App (Update A)**

High level vulnerability: Use of Hard-coded Credentials.

Enphase Installer Toolkit Android App (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 2023 July:

CISA and Partners Release Joint Cybersecurity Advisory on Newly Identified Truebot Malware Variants

stopransomware; Increased Truebot Activity Infects U.S. and Canada Based Networks; implement the recommended mitigations;

Link and more information:

CISA and Partners Release Joint Cybersecurity Advisory on Newly Identified Truebot Malware Variants | CISA

Mozilla Releases Security Update for Firefox and Firefox ESR

Firefox and Firefox ESR; vulnerability management; Mozilla Security Advisory;

Link and more information:

Mozilla Releases Security Update for Firefox and Firefox ESR | CISA

CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting Outlook Online

Microsoft Exchange Online Microsoft 365 Minimum Viable Secure Configuration Baselines; Secure Cloud Business Applications; provide guidance to agencies and critical infrastructure organizations;

Link and more information:

CISA and FBI Release Cybersecurity Advisory on Enhanced Monitoring to Detect APT Activity Targeting Outlook Online | CISA

CISA Develops Factsheet for Free Tools for Cloud Environments

Free Tools for Cloud Environments; Cybersecurity Evaluation Tool (CSET); Secure Cloud Business Applications (SCuBA) Gear;

Link and more information:

CISA Develops Factsheet for Free Tools for Cloud Environments | CISA

NSA, CISA Release Guidance on Security Considerations for 5G Network Slicing

5G Network Slicing: Security Considerations for Design, Deployment, and Maintenance; Potential Threats to 5G Network Slicing;

Link and more information:

NSA, CISA Release Guidance on Security Considerations for 5G Network Slicing | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-36884 Microsoft Office and Windows HTML Remote Code Execution Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CVE-2023-29298 Adobe ColdFusion Improper Access Control Vulnerability; CVE-2023-38205 Adobe ColdFusion Improper Access Control Vulnerability;

Link and more information:

CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Releases Cybersecurity Advisory on Threat Actors Exploiting Citrix CVE-2023-3519

Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells; unauthenticated remote code execution (RCE) vulnerability affecting NetScaler (formerly Citrix) Application Delivery Controller (ADC);

Link and more information:

CISA Releases Cybersecurity Advisory on Threat Actors Exploiting Citrix CVE-2023-3519 | CISA

Atlassian Releases Security Updates

Address vulnerabilities in Confluence Data Center & Server (CVE-2023-22505 and CVE-2023-22508) and Bamboo Data Center (CVE-2023-22506;

Link and more information:

Atlassian Releases Security Updates | CISA

Ivanti Releases Security Updates for Endpoint Manager Mobile (EPMM) CVE-2023-35078

This vulnerability (CVE-2023-35078) affects supported EPMM versions 11.10, 11.9, and 11.8. Older, unsupported versions are also affected;

Link and more information:

Ivanti Releases Security Updates for Endpoint Manager Mobile (EPMM) CVE-2023-35078 | CISA

Apple Releases Security Updates for Multiple Products

iOS 16.6 and iPadOS 16.6; iOS 15.7.8 and iPadOS 15.7.8; macOS Ventura 13.5; macOS Monterey 12.6.8; macOS Big Sur 11.7.9; Safari 16.6; tvOS 16.6; watchOS 9.6,

Link and more information:

Apple Releases Security Updates for Multiple Products | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-35078 Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-38606 Apple Multiple Products Kernel Unspecified Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Releases Analysis of FY22 Risk and Vulnerability Assessments

Analysis and infographic detailing the findings from the 121 Risk and Vulnerability Assessments (RVAs) conducted across multiple critical infrastructure sectors in fiscal year 2022 (FY22);

Link and more information:

CISA Releases Analysis of FY22 Risk and Vulnerability Assessments | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-37580 Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA and Partners Release Joint Cybersecurity Advisory on Preventing Web Application Access Control Abuse

Preventing Web Application Access Control Abuse, to warn vendors, designers, developers, and end-user organizations of web applications about insecure direct object reference (IDOR) vulnerabilities;

Link and more information:

CISA and Partners Release Joint Cybersecurity Advisory on Preventing Web Application Access Control Abuse | CISA

Ivanti Releases Security Updates for EPMM to address CVE-2023-35081

Ivanti has identified and released patches for a directory traversal vulnerability (CVE-2023-35081, CWE-22) in Ivanti Endpoint Manager Mobile (EPMM);

Link and more information:

Ivanti Releases Security Updates for EPMM to address CVE-2023-35081 | CISA

CISA Releases Malware Analysis Reports on Barracuda Backdoors

CISA has published three malware analysis reports on malware variants associated with exploitation of CVE-2023-2868;

Link and more information:

CISA Releases Malware Analysis Reports on Barracuda Backdoors | CISA