2023 October, 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

Best Practices for Upgrading SCADA Software and Systems

CDW published an article with SCADA security best practices. This short recommendation summarizes the important things.

The overall cybersecurity landscape has shifted dramatically in recent years, with security professionals reporting an increase in both the volume and sophistication of threats facing their organizations. This means that those who are launching attacks on SCADA networks are almost certainly leveraging techniques and tools that are more advanced than the ones available when these networks were set up. In particular, the emergence of advanced persistent threats and the increasing prevalence of ransomware and industrial espionage pose substantial risks to SCADA networks.

To defend against these evolving threats, organizations must adopt a proactive and multilayered approach to their SCADA network security. This includes:

- Regular risk assessments and vulnerability scanning
- Robust access controls and user authentication mechanisms
- Secure network segmentation
- Real-time network traffic monitoring

Additionally, organizations should prioritize regular patching and updating of SCADA systems and conduct ongoing security awareness training for their employees.

Source and more information available on the following link:

https://www.cdw.com/content/cdw/en/articles/networking/protecting-scada-networks-in-an-evolving-threat-landscape.html

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in November 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/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

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

New in this feed!

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

10th Annual Control Systems Cybersecurity Europe and UK

The Cyber Senate Control Systems Cybersecurity UK EU conference provides the energy, manufacturing, transport, power and industrial sectors with the opportunity to learn from their peers and together, define their priorities, close the gap of disconnect between people and technology and reinforce their mission from a reactive to proactive state of cyber security. Attended by leading Subject Matter Experts from the asset owner, technology and government sphere, this years focus will be on sharing collective experiences that can help organisations design and implement their transition plan to zero trust architecture, better manage IT and OT convergence, improve technology selection and how to develop partnerships that foster growth and help manage risk – faster. Attendees will not only gain a clearer picture of OT cyber risk, but learn how others in their field have fixed it.

London, United Kingdom; 07th – 08th November 2023

More details can be found on the following website:

https://industrialcyber.co/event/9th-annual-control-systems-cyber-security-europe-and-uk/

Industrial Security Conference in Copenhagen

There are 16 critical infrastructure sectors whose assets, systems and networks are considered so vital that their destruction have a damaging effect on security, economic security, public health, and safety. The energy sector is one of the main targets of cyber-attacks and hacking against critical infrastructure, but it is not the only one. Transport, public sector services, telecommunications and critical manufacturing industries are also targets. It is especially dangerous and costly because it disrupts necessities such as water, heat, healthcare, and food supply. At ISC-CPH in Copenhagen 13-14-15 November 2023, you will experience presentations from leading experts around the world, rewarding keynotes, knowledge sharing and networking with international peers in the industry.

Copenhagen, Denmark; 13th – 15th November 2023

More details can be found on the following website:

https://industrialcyber.co/event/industrial-security-conference-in-copenhagen/

Palo Alto Networks Industrial OT Security Hands-On Workshops

OT assets in industrial organizations are vulnerable and exposed. Gartner predicts that by 2025, 30% of organizations in the industrial sector will experience a security breach that will halt operations or impact mission-critical cyber-physical systems.

Join the Industrial OT Security hands-on workshop and gain firsthand experience on how to protect your OT assets and networks.

In this hands-on workshop, you'll learn in a live lab how to:

- Know and assess your OT threat surface with accurate asset visibility and extensive OT asset vulnerability and risk assessment
- Visualize your OT assets and communication patterns mapped to the Purdue Model
- Protect the OT perimeter and assets with granular segmentation using OT device context and OT/ICS process integrity

Online (Virtual); 14th November 2023

More details can be found on the following website:

https://industrialcyber.co/event/palo-alto-networks-industrial-ot-security-hands-on-workshops-november/

Annual Cyber & SCADA Security for Power and Utilities

The 10th Cyber & SCADA Security Conference is a premier event dedicated to exploring the latest advancements, challenges, and best practices in the field of cybersecurity for Critical Infrastructure Systems and Supervisory Control and Data Acquisition (SCADA) systems. This conference brings together leading experts, researchers, industry professionals, and government officials from around the world to discuss and share their knowledge and experiences.

The conference welcomes professionals and researchers involved in the cybersecurity of Critical Infrastructure Systems and SCADA systems. This includes, but is not limited to, cybersecurity professionals, SCADA operators, IT managers, system administrators, government officials, researchers, and academicians.

Berlin, Germany; 23rd – 24th November 2023

More details can be found on the following website:

https://industrialcyber.co/event/cyber-scada-security-for-power-and-utilities/

Cyber Security for Critical Assets Conference: The Digitalisation of Critical Infrastructures

The MENA region is considered one of the world's most targeted regions for cyber-attacks, largely due to its rising populations, pre-existing political tensions and major industrial projects which are driving the next levels of innovation and digitalisation that aim to transform the future of the region. Although the region strives to be front-runners in digital innovation, the level of security maturity must be improved if they are to achieve this goal.

As OT environments continue to converge with IT networks the need to secure these technologies to support continuous uptime and safety, has never been more critical. In particular, for business leaders in the Oil & Gas, Chemical, Healthcare, Mining, Utility, Maritime, and other critical industries.

With this in mind, CS4CA MENA summit will explore all aspects of IT & OT security with a focus on digitally transforming critical infrastructures. The summit will bring together some of the brightest minds in the industry, uniting 100+ IT & OT security leaders in Riyadh for 2 days of insight building, strategy planning and expert knowledge exchange on November 2023.

Riyadh, Saudi Arabia; 28th – 29th November 2023

More details can be found on the following website:

https://industrialcyber.co/event/cyber-security-for-critical-assets-cs4ca-mena/

ICS incidents

Gaza-Linked Cyber Threat Actor Targets Israeli Energy and Defense Sectors

A Gaza-based threat actor, known as Storm-1133, has been identified as the perpetrator behind a series of cyberattacks targeting Israeli private-sector energy, defense, and telecommunications organizations, according to Microsoft's fourth annual Digital Defense Report.

Microsoft attributes the activities of Storm-1133 to further the interests of Hamas, a Sunni militant group that governs the Gaza Strip. The cyber campaign primarily focuses on organizations perceived as hostile to Hamas, including Israeli energy and defense sectors, as well as entities loyal to Fatah, a Palestinian political party based in the West Bank.

The attack strategy employed by Storm-1133 combines social engineering tactics and fake LinkedIn profiles posing as Israeli human resources managers, project coordinators, and software developers. These deceptive personas are used to contact employees at Israeli organizations, conduct reconnaissance, and deliver phishing messages and malware.

Furthermore, Microsoft has observed Storm-1133 attempting to infiltrate third-party organizations with public ties to Israeli targets. This infiltration includes deploying backdoors and maintaining a command-and-control infrastructure hosted on Google Drive, allowing the threat actors to dynamically update their operations and evade static network-based defenses.

This revelation comes amidst an escalation in the Israeli-Palestinian conflict, marked by a surge in hacktivist operations such as "Ghosts of Palestine," targeting government websites and IT systems in Israel, the U.S., and India. Asian hacktivist groups have been particularly active in these incidents, with their motivations largely tied to their alignment with the U.S.

In addition, nation-state cyber threats have shifted from destructive to long-term espionage campaigns. The report highlights the increased sophistication of Iranian and North Korean state actors in their cyber operations, noting that they are closing the gap with cyber actors from Russia and China. These actors employ custom tools and backdoors to maintain persistence, evade detection, and steal credentials.

In summary, Storm-1133, a Gaza-linked cyber threat actor, has been targeting Israeli energy and defense sectors using a combination of social engineering tactics and fake LinkedIn profiles. This cyber threat comes at a time of increased hacktivist activity and evolving nation-state cyber threats, with Iran and North Korea showing notable advancements in their cyber operations.

The source is available on the following link:

https://thehackernews.com/2023/10/gaza-linked-cyber-threat-actor-targets.html

Book recommendation

How to Be OT Cybersecurity Professional

It's a bitter truth that we live in an age of vulnerable systems, where our existence is completely dependent on them. Cyber attacks can cause greater damage than actual war losses for a country that is unprepared for them. After several incidents that impacted social order, governments have realized this fact.

During a cyber attack, the city will be paralyzed, food supply will be interrupted, and medical care will be disrupted. There would be human casualties and the worst of the people would emerge if fuel or electricity were unavailable.

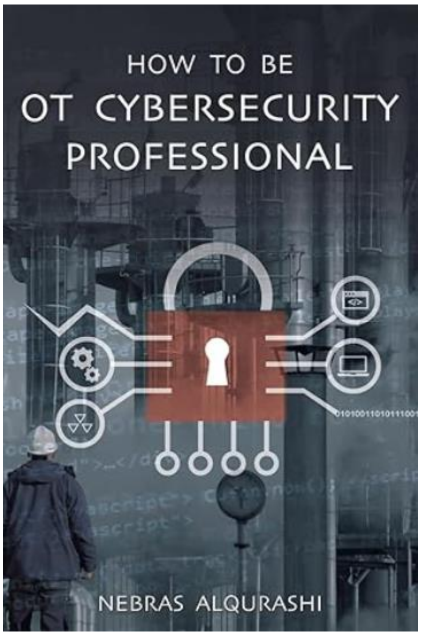
The age of cyber missiles has arrived, and as Dale Peterson pointed out, our infrastructure systems are insecure by design. We need to learn how to secure all operational technology, it's crucial, and it can only be done by understanding the bits and bytes of these operations. In this book, you'll learn Cybersecurity for Operational Technology, how to secure all types of Operational Technology, and how to save lives!

Author/Editor: Nebras Alqurashi (Author)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/How-Be-OT-Cybersecurity-Professional/dp/9948789202



ICS security news selection

DHS: Physical Security a Concern in Johnson Controls Cyberattack

In the latest development around the cyberattack impacting Johnson Controls International (JIC), officials at the Department of Homeland Security (DHS) are now reportedly concerned that the attack may have affected sensitive physical security information.

Johnson Controls serves as a government contractor, providing building automation services to facilities, such as HVAC, fire, and security equipment. Due to the nature of those services, officials at DHS are raising concerns about compromised information such as DHS floor plans. According to media reports, officials detailed in an internal memo that Johnson Controls holds "classified/sensitive contracts for DHS that depict the physical security of many DHS facilities.". …

Source, and more information:

https://www.darkreading.com/ics-ot/dhs-physical-security-concern-johnson-controls-cyberattack

NIST Publishes Final Version of 800-82r3 OT Security Guide

NIST has published the final version of the SP 800-82 Revision 3 guide to operational technology (OT) security.

The 316-page document provides guidance on improving the security of OT systems while addressing their unique safety, reliability and performance requirements.

“SP 800-82r3 provides an overview of OT and typical system topologies, identifies typical threats to organizational mission and business functions supported by OT, describes typical vulnerabilities in OT, and provides recommended security safeguards and countermeasures to manage the associated risks,” NIST explained.

Source, and more information:

https://www.securityweek.com/nist-publishes-final-version-of-800-82r3-ot-security-guide/

Legions of Critical Infrastructure Devices Subject to Cyber Targeting

There are at least 100,000 industrial control systems (ICS) exposed to the public Internet around the world, controlling a host of critical operational technologies (OT) like power grids, water systems, and building management systems (BMS). While that's a big number, researchers note that quantifying true cyber-risk from that exposure means examining which protocols the gear uses.

In a recent analysis, researchers from cyber-risk handicapper Bitsight reached the 100,000 number by inventorying reachable devices that use the top 10 most popular and widely used ICS protocols (including Modbus, KNX, BACnet, Niagara Fox, and others.)

Source, and more information:

https://www.darkreading.com/ics-ot/legions-critical-infrastructure-devices-open-cyber-targeting

Addressing cyber threats in healthcare operational technology

The proliferation of connected medical devices (IoMT) in hospitals demands a holistic approach to cybersecurity beyond just the digital IT realm. Industrial cybersecurity (OT) requires integrated solutions to address its unique challenges.

In this Help Net Security video, Estefanía Rojas Campos, OT Security Specialist at Entelgy Innotec Security, discusses securing cyber-physical environments and offers insight on ensuring cybersecurity in hospitals. …

Source, and more information:

https://www.helpnetsecurity.com/2023/10/19/cyber-threats-healthcare-ot-video/

Milesight Industrial Router Vulnerability Possibly Exploited in Attacks

A vulnerability affecting some industrial routers made by Chinese IoT and video surveillance product maker Milesight may have been exploited in attacks, according to exploit and vulnerability intelligence firm VulnCheck.

Several UR-series industrial cellular routers from Milesight (Ursalink) are affected by CVE-2023-43261, a serious vulnerability exposing system log files, such as ‘httpd.log’.

The exposed logs contain passwords for administrators and other users, which can be leveraged by remote, unauthenticated attackers to gain unauthorized access to the targeted device. The passwords are not stored in plain text in the log files, but they can be easily cracked. …

Source, and more information:

https://www.securityweek.com/milesight-industrial-router-vulnerability-possibly-exploited-in-attacks/

What is operational risk and why should you care? Assessing SEC rule readiness for OT and IoT

The newly released Security and Exchange Commission (SEC) cyber incident disclosure rules have been met with mixed reviews. Of particular concern is whether public companies who own and operate industrial control systems and connected IoT infrastructure are prepared to fully define operational risk, and therefore are equipped to fully disclose material business risk from cyber incidents. This concern also provides a fresh opportunity for preparedness.

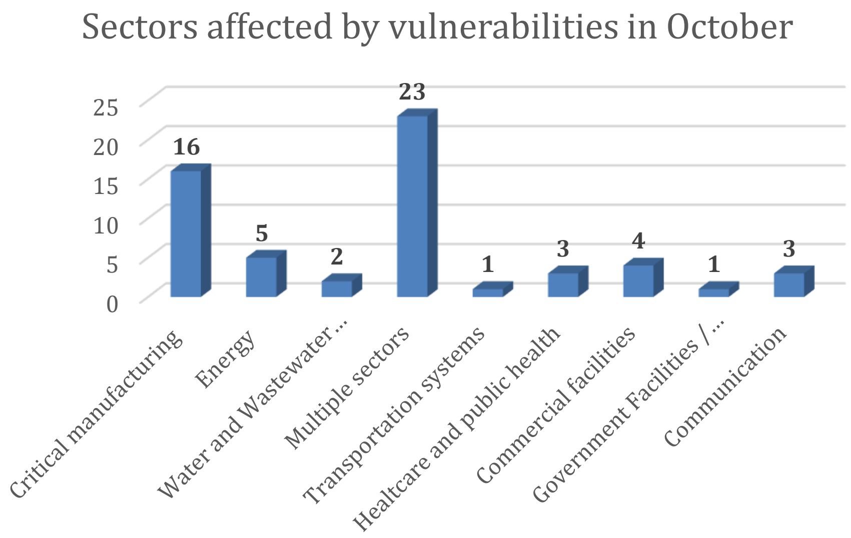
The rules require registrants to disclose material cybersecurity incidents (via an 8-K filing) no later than four business days after determining that the incident is material. Additionally, the rules require public companies to annually disclose information regarding their cybersecurity risk management and governance strategy for assessing, identifying and managing material cybersecurity risks as part of their 10-K filing. …

Source, and more information:

https://www.helpnetsecurity.com/2023/10/25/operational-risk/

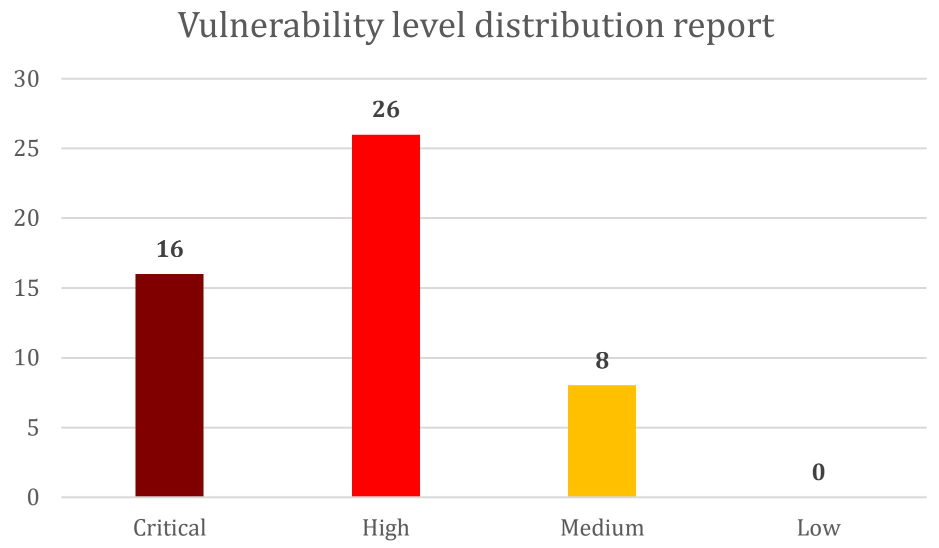
ICS vulnerabilities

In October 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 and Siemens ProductCERT and Siemens CERT:



The most common vulnerabilities in October:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	8
Out-of-bounds Read	CWE-125	6
Improper Access Control	CWE-284	5
Improper Authentication	CWE-287	4
Stack-based Buffer Overflow	CWE-121	4



ICSA-23-304-02: **INEA ME RTU**

Critical level vulnerabilities: OS Command Injection, Improper Authentication.

[INEA ME RTU | CISA]

ICSA-23-304-03: **Zavio IP Camera**

Critical level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, OS Command Injection.

[Zavio IP Camera | CISA]

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

Critical level vulnerability: Classic Buffer Overflow.

[Mitsubishi Electric CNC Series (Update B) | CISA]

ICSA-23-299-01: **Dingtian DT-R002**

Medium level vulnerability: Authentication Bypass by Capture-Replay.

[Dingtian DT-R002 | CISA]

ICSA-23-299-02: **Centralite Pearl Thermostat**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

[Centralite Pearl Thermostat | CISA]

ICSA-23-299-03: **Ashlar-Vellum Cobalt, Graphite, Xenon, Argon, Lithium**

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

Ashlar-Vellum Cobalt, Graphite, Xenon, Argon, Lithium | CISA

ICSA-23-299-04: **Rockwell Automation Arena**

High level vulnerabilities: Out-of-Bounds Read, Access of Uninitialized Pointer.

Rockwell Automation Arena | CISA

ICSA-23-299-05: **Rockwell Automation FactoryTalk View Site Edition**

High level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk View Site Edition | CISA

ICSA-23-299-06: **Rockwell Automation FactoryTalk Services Platform**

High level vulnerability: Improper Authentication.

Rockwell Automation FactoryTalk Services Platform | CISA

ICSA-23-299-07: **Sielco PolyEco FM Transmitter**

Critical level vulnerabilities: Session Fixation, Improper Restriction of Excessive Authentication Attempts, Improper Access Control.

Sielco PolyEco FM Transmitter | CISA

ICSA-23-299-08: **Sielco Radio Link and Analog FM Transmitters**

Critical level vulnerabilities: Improper Access Control, Cross-Site Request Forgery, Privilege Defined with Unsafe Actions.

Sielco Radio Link and Analog FM Transmitters | CISA

ICSMA-23-194-01: **BD Alaris System with Guardrails Suite MX (Update A)**

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 (Update A) | CISA

ICSA-23-297-01: **Rockwell Automation Stratix 5800 and Stratix 5200**

Critical level vulnerability: Unprotected Alternate Channel.

Rockwell Automation Stratix 5800 and Stratix 5200 | CISA

ICSA-23-143-02: **Hitachi Energy's RTU500 Series Product (UPDATE B)**

Critical level vulnerabilities: Type Confusion, Observable Timing Discrepancy, Out-of-bounds Read, Infinite Loop, Classic Buffer Overflow.

Hitachi Energy's RTU500 Series Product (Update B) | CISA

ICSA-23-290-01: **Schneider Electric EcoStruxure Power Monitoring Expert and Power Operation Products**

Critical level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Monitoring Expert and Power Operation Products | CISA

ICSA-23-290-02: **Rockwell Automation FactoryTalk Linx**

High level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk Linx | CISA

SSA-712929: **Siemens Industrial Products (Update: 2.4.)**

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

SSA-712929 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update: 1.1.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-710008: **Siemens SCALANCE Products (Update: 1.4.)**

Critical level vulnerabilities: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Allocation of Resources Without Limits or Throttling, Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS).

SSA-710008 (siemens.com)

SSA-516174: **Siemens SCALANCE W1750D (Update: 1.1.)**

High level vulnerability: Improper Input Validation.

SSA-516174 (siemens.com)

SSB-439005: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP (Update: 5.6.)**

Medium level vulnerabilities: Multiple vulnerabilities.

SSB-439005 (siemens.com)

SSA-413565: **Siemens SCALANCE Products** **(Update: 1.3.)**

High level vulnerabilities: Improper Control of Generation of Code ('Code Injection'), Use of a Broken or Risky Cryptographic Algorithm, Storing Passwords in a Recoverable Format, Improper Validation of Specified Quantity in Input, Improper Control of a Resource Through its Lifetime.

SSA-413565 (siemens.com)

SSA-363107: **Siemens SIMATIC WinCC** **(Update: 1.3.)**

High level vulnerability: Insecure Default Initialization of Resource.

SSA-363107 (siemens.com)

SSA-285795: **Siemens Industrial Products** **(Update: 1.4.)**

Medium level vulnerability: NULL Pointer Dereference.

SSA-285795 (siemens.com)

SSA-250085: **Siemens SINEC NMS and SINEMA Server** **(Update: 1.3.)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Deserialization of Untrusted Data, Improper Privilege Management.

SSA-250085 (siemens.com)

SSA-240541: **Siemens WIBU Systems CodeMeter** **(Update: 1.1.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-240541 (siemens.com)

SSA-203374: **Siemens Multiple OpenSSL Vulnerabilities in SCALANCE W1750D Devices** **(Update: 1.1.)**

High level vulnerability: Improper Input Validation.

SSA-203374 (siemens.com)

ICSA-23-285-01: **Siemens SIMATIC CP products**

High level vulnerabilities: Improper Access Control, Uncontrolled Resource Consumption.

Siemens SIMATIC CP products | CISA

ICSA-23-285-02: **Siemens SCALANCE W1750D**

Critical level vulnerabilities: Classic Buffer Overflow, Command Injection, Exposure of Sensitive Information to an Unauthorized Actor.

Siemens SCALANCE W1750D | CISA

ICSA-23-285-03: **Siemens SICAM A8000 Devices**

High level vulnerability: Path Traversal.

Siemens SICAM A8000 Devices | CISA

ICSA-23-285-04: **Siemens Xpedition Layout Browser**

High level vulnerability: Stack-Based Buffer Overflow.

Siemens Xpedition Layout Browser | CISA

ICSA-23-285-05: **Siemens Simcenter Amesim**

High level vulnerability: Code Injection.

Siemens Simcenter Amesim | CISA

ICSA-23-285-06: **Siemens SICAM PAS/PQS**

Medium level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SICAM PAS/PQS | CISA

ICSA-23-285-07: **Siemens RUGGEDCOM APE180**

High level vulnerabilities: SQL Injection, Cross-site Scripting, Improper Input Validation, Incorrect Authorization, Session Fixation.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-23-285-08: **Siemens SINEC NMS**

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

Siemens SINEC NMS | CISA

ICSA-23-285-09: **Siemens CPCI85 Firmware of SICAM A8000 Devices**

Critical level vulnerability: Use of Hard-coded Credentials.

Siemens CPCI85 Firmware of SICAM A8000 Devices | CISA

ICSA-23-285-10: **Siemens Tecnomatix Plant Simulation**

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

Siemens Tecnomatix Plant Simulation | CISA

ICSA-23-285-11: **Siemens Mendix Forgot Password Module**

Medium level vulnerability: Observable Discrepancy.

Siemens Mendix Forgot Password Module | CISA

ICSA-23-285-12: **Weintek cMT3000 HMI Web CGI**

Critical level vulnerabilities: Stack-based Buffer Overflow, OS Command Injection.

Weintek cMT3000 HMI Web CGI | CISA

ICSA-23-285-13: **Mitsubishi Electric MELSEC-F Series**

Critical level vulnerability: Improper Authentication.

Mitsubishi Electric MELSEC-F Series | CISA

ICSA-23-285-14: **Hikvision Access Control and Intercom Products**

High level vulnerabilities: Session Fixation, Improper Access Control.

Hikvision Access Control and Intercom Products | CISA

ICSA-23-285-15: **Advantech WebAccess**

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

Advantech WebAccess | CISA

ICSA-23-285-16: **Schneider Electric IGSS**

High level vulnerability: Missing Authentication for Critical Function.

Schneider Electric IGSS | CISA

ICSMA-23-285-01: **Santesoft Sante DICOM Viewer Pro**

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

Santesoft Sante DICOM Viewer Pro | CISA

ICSMA-23-285-02: **Santesoft Sante FFT Imaging**

High level vulnerability: Out-of-Bounds Read.

Santesoft Sante FFT Imaging | CISA

ICSA-23-243-03: **PTC Kepware KepServerEX (Update A)**

Medium level vulnerabilities: Uncontrolled Search Path Element, Improper Input Validation, Insufficiently Protected Credentials.

PTC Kepware KepServerEX (Update A) | CISA

ICSA-19-029-02: **Mitsubishi Electric MELSEC-Q Series PLCs CISA (Update A)**

High level vulnerability: Resource Exhaustion.

Mitsubishi Electric MELSEC-Q Series PLCs (Update A) | CISA

ICSA-23-278-01: **Hitachi Energy AFS65x, AFF66x, AFS67x, and AFR67x Series Products**

Critical level vulnerabilities: Incorrect Calculation, Integer Overflow or Wraparound, Improper Encoding or Escaping of Output, Exposure of Resource to Wrong Sphere.

Hitachi Energy AFS65x, AFF66x, AFS67x, and AFR67x Series Products | CISA

ICSA-23-278-02: **Qognify NiceVision**

Critical level vulnerability: Use of Hard-coded Credentials.

Qognify NiceVision | CISA

ICSA-23-278-03: **Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch**

Medium level vulnerabilities: Observable Timing Discrepancy, Double Free.

Mitsubishi Electric CC-Link IE TSN Industrial Managed Switch | 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 October:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-5217 Google Chrome libvpx Heap Buffer Overflow Vulnerability;
CVE-2023-4211 Arm Mali GPU Kernel Driver Use-After-Free Vulnerability;
CVE-2023-42793 JetBrains TeamCity Authentication Bytás Vulnerability;
CVE-2023-28229 Microsoft Windows CNG Key Isolation Service Privilege Escalation Vulnerability;
CVE-2023-40044 Progress WS_FTP Server Deserialization of Untrusted Data Vulnerability ;
CVE-2023-42824 Apple iOS and iPadOS Kernel Privilege Escalation Vulnerability
CVE-2023-22515 Atlassian Confluence Data Center and Server Privilege Escalation Vulnerability;
CVE-2023-21608 Adobe Acrobat and Reader Use-After-Free Vulnerability;
CVE-2023-20109 Cisco IOS and IOS XE Group Encrypted Transport VPN Out-of-Bounds Write Vulnerability;
CVE-2023-41763 Microsoft Skype for Business Privilege Escalation Vulnerability;
CVE-2023-36563 Microsoft WordPad Information Disclosure Vulnerability;
CVE-2023-44487 HTTP/2 Rapid Reset Attack Vulnerability;
CVE-2023-20198 Cisco IOS XE Web UI Privilege Escalation Vulnerability;
CVE-2023-4966 Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability;
CVE-2021-1435 Cisco IOS XE Web UI Command Injection Vulnerability;
CVE-2023-20273 Cisco IOS XE Web UI Unspecified Vulnerability;
CVE-2023-5631 Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability;
CVE-2023-46747 F5 BIG-IP Authentication Bypass Vulnerability;
CVE-2023-46748 F5 BIG-IP SQL Injection Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog, Removes Five KEVs | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known 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 One Known Exploited Vulnerability to Catalog | CISA

CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA and NSA Release New Guidance on Identity and Access Management

CISA and the National Security Agency (NSA) published Identity and Access Management: Developer and Vendor Challenges, authored by the Enduring Security Framework (ESF), a CISA- and NSA-led working panel that includes a public-private cross-sector partnership. ESF aims to address risks that threaten critical infrastructure and national security systems.

Link and more information:

CISA and NSA Release New Guidance on Identity and Access Management | CISA

Cisco Releases Security Advisories for Multiple Products

Cisco released security advisories for vulnerabilities affecting multiple Cisco products. A remote cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Link and more information:

Cisco Releases Security Advisories for Multiple Products | CISA

Atlassian Releases Security Advisory for Confluence Data Center and Server

Atlassian released a security advisory to address a vulnerability affecting Confluence Data Center and Confluence Server. A remote cyber threat actor could exploit this vulnerability to take control of an affected system.

Link and more information:

Atlassian Releases Security Advisory for Confluence Data Center and Server | CISA

NSA and CISA Release Advisory on Top Ten Cybersecurity Misconfigurations

National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) released a joint cybersecurity advisory (CSA), NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations, which provides the most common cybersecurity misconfigurations in large organizations, and details the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

Link and more information:

NSA and CISA Release Advisory on Top Ten Cybersecurity Misconfigurations | CISA

Apple Releases Security Updates for iOS and iPadOS

Apple has released security updates to address vulnerabilities in iOS and iPadOS. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.

Link and more information:
Apple Releases Security Updates for iOS and iPadOS | CISA

CISA, FBI, NSA, and Treasury Release Guidance on OSS in IT/ICS Environments
CISA, the Federal Bureau of Investigation, the National Security Agency, and the U.S. Department of the Treasury released guidance on improving the security of open source software (OSS) in operational technology (OT) and industrial control systems (ICS).
Link and more information:
CISA, FBI, NSA, and Treasury Release Guidance on OSS in IT/ICS Environments | CISA

HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487
Researchers and vendors have disclosed a denial-of-service (DoS) vulnerability in HTTP/2 protocol. The vulnerability (CVE-2023-44487), known as Rapid Reset, has been exploited in the wild in August 2023 through October 2023.
Link and more information:
HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487 | CISA

Citrix Releases Security Updates for Multiple Products
Citrix has released security updates to address vulnerabilities affecting multiple products. A malicious cyber actor can exploit one of these vulnerabilities take control of an affected system.
Link and more information:
Citrix Releases Security Updates for Multiple Products | CISA

Microsoft Releases October 2023 Security Updates
Microsoft has released updates to address multiple vulnerabilities in Microsoft software. A cyber threat actor can exploit some of these vulnerabilities to take control of an affected system.
Link and more information:
Microsoft Releases October 2023 Security Updates | CISA

FBI and CISA Release Update on AvosLocker Advisory
Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA), #StopRansomware: AvosLocker Ransomware (Update) to disseminate known indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), and detection methods associated with the AvosLocker variant identified through FBI investigations as recently as May 2023.

Link and more information:
[FBI and CISA Release Update on AvosLocker Advisory | CISA]

Fortinet Releases Security Updates for Multiple Products
Fortinet has released security advisories addressing vulnerabilities in multiple products. These vulnerabilities may allow cyber threat actors to take control of the affected systems.
Link and more information:
[Fortinet Releases Security Updates for Multiple Products | CISA]

CISA Releases New Resources Identifying Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware
CISA launched two new resources for combating ransomware campaigns:
A "Known to be Used in Ransomware Campaigns" column in the KEV Catalog that identifies KEVs associated with ransomware campaigns.
A "Misconfigurations and Weaknesses Known to be Used in Ransomware Campaigns" table on StopRansomware.gov that identifies misconfigurations and weaknesses associated with ransomware campaigns. The table features a column that identifies the Cyber Performance Goal (CPG) action for each misconfiguration or weakness.
Link and more information:
[CISA Releases New Resources Identifying Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware | CISA]

CISA, FBI, and MS-ISAC Release Joint Advisory on Atlassian Confluence Vulnerability CVE-2023-22515
CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA) in response to the active exploitation of CVE-2023-22515.
Link and more information:
[CISA, FBI, and MS-ISAC Release Joint Advisory on Atlassian Confluence Vulnerability CVE-2023-22515 | CISA]

Cisco Releases Security Advisory for IOS XE Software Web UI
Cisco released a security advisory to address a vulnerability (CVE-2023-20198) affecting IOS XE Software Web UI. A cyber threat actor can exploit this vulnerability to take control of an affected device.
Link and more information:

[Cisco Releases Security Advisory for IOS XE Software Web UI | CISA]

CISA, NSA, FBI, and MS-ISAC Release Phishing Prevention Guidance

Cybersecurity Infrastructure and Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint guide, Phishing Guidance: Stopping the Attack Cycle at Phase One.

Link and more information:

[CISA, NSA, FBI, and MS-ISAC Release Phishing Prevention Guidance | CISA]

CISA, NSA, FBI, and MS-ISAC Release Update to #StopRansomware Guide

Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released an updated version of the joint #StopRansomware Guide.

Link and more information:

[CISA, NSA, FBI, and MS-ISAC Release Update to #StopRansomware Guide | CISA]

Oracle Releases October 2023 Critical Patch Update Advisory

Oracle has released its Critical Patch Update Advisory for October 2023 to address 387 vulnerabilities across multiple products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Link and more information:

[Oracle Releases October 2023 Critical Patch Update Advisory | CISA]

CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities

CISA updated its guidance addressing two vulnerabilities, CVE-2023-20198 and CVE-2023-20273, affecting Cisco's Internetworking Operating System (IOS) XE Software Web User Interface (UI).

Link and more information:

[CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities | CISA]

Mozilla Releases Security Advisories for Multiple Products

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

Link and more information:

Mozilla Releases Security Advisories for Multiple Products | CISA

Apple Releases Security Advisories for Multiple Products

Apple 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 device.

Link and more information:

Apple Releases Security Advisories for Multiple Products | CISA

VMware Releases Security Advisory for vCenter Server

VMware released a security advisory for vulnerabilities (CVE-2023-34048, CVE-2023-34056) affecting the VMware vCenter Server.

Link and more information:

VMware Releases Security Advisory for vCenter Server | CISA

CISA Announces Launch of Logging Made Easy

CISA announces the launch of a new version of Logging Made Easy (LME), a straightforward log management solution for Windows-based devices that can be downloaded and self-installed for free.

Link and more information:

CISA Announces Launch of Logging Made Easy | CISA

CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities With Additional Releases

CISA updated its guidance addressing two vulnerabilities, CVE-2023-20198 and CVE-2023-20273, affecting Cisco's Internetworking Operating System (IOS) XE Software Web User Interface (UI).

Link and more information:

CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities With Additional Releases | CISA

VMware Releases Advisory for VMware Tools Vulnerabilities

VMware released a security advisory addressing multiple vulnerabilities (CVE-2023-34057, CVE-2023-34058) in VMware Tools. A cyber actor could exploit one of these vulnerabilities to take control of an affected system.

Link and more information:

VMware Releases Advisory for VMware Tools Vulnerabilities | CISA