2023 November, 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

MITRE ATT&CK v14 released

MITRE has released MITRE ATT&CK v14, an updated version of its renowned cyberattack investigation framework. ATT&CK's primary objective is to document and classify behaviours exhibited by cyber adversaries during real-world attacks. The framework continuously evolves to encompass new and altered attacker behaviours related to their interactions with devices, systems, and networks.

MITRE ATT&CK v14 covers multiple matrices, including Enterprise (targeting Windows, macOS, Linux, PRE, cloud platforms, networking devices, and containers), Mobile (Android and iOS), and ICS (industrial control systems). The latest release has broadened its scope to include activities closely associated with direct network interactions or impacts. This expansion involves deceptive practices and social engineering techniques such as Financial Theft, Impersonation, and Spearphishing.

Additional enhancements in MITRE ATT&CK v14 include improved detection notes to aid in identifying adversary behaviours when analyzing network traffic, strengthened connections between detections, data sources, and mitigations, and the incorporation of new assets in the ICS matrix. The Mobile matrix now has an extended scope, adding new phishing vectors, including "quishing," and structured detections. The release also introduces new software, attack groups, and documented campaigns.

MITRE ATT&CK is updated biannually and has evolved from a basic Excel spreadsheet identifying adversaries and tactics into a globally recognized framework that users worldwide reference and contribute to. Organizations can utilize this framework to refine their threat models, assess vendor capabilities, map detections to streamline analyst tasks, enhance employee education, and more. Implementation should start gradually, focusing on specific tactics relevant to an organization's system. This approach allows organizations to identify potential threats and apply protective measures effectively.

MITRE is also working on D3FEND, a complementary knowledge base of defensive countermeasures for common offensive techniques, to supplement the ATT&CK framework.

Source and more information available on the following link:

https://www.helpnetsecurity.com/2023/11/02/mitre-attck-v14/

ICS trainings, education

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

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

Annual Computer Security Applications Conference (ACSAC) 2023

The Annual Computer Security Applications Conference (ACSAC) brings together cutting-edge researchers, with a broad cross-section of security professionals drawn from academia, industry, and government, gathered to present and discuss the latest security results and topics. With peer reviewed technical papers, invited talks, panels, national interest discussions, and workshops, ACSAC continues its core mission of investigating practical solutions for computer and network security technology.

Austin, Texas USA; 03rd – 04th December 2023

More details can be found on the following website:

https://www.acsac.org/

17. International Conference on Critical Infrastructure Resilience and Protection

International Conference on Critical Infrastructure Resilience and Protection aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Critical Infrastructure Resilience and Protection. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Critical Infrastructure Resilience and Protection.

Barcelona, Spain; 18th – 19th December 2023

More details can be found on the following website:

https://waset.org/critical-infrastructure-resilience-and-protection-conference-in-december-2023-in-barcelona?utm_source=conferenceindex&utm_medium=referral&utm_campaign=listing

ICS incidents

Boeing Investigating Cyber Incident

Boeing has confirmed a cyber incident that has impacted its parts and distribution business. The incident was previously claimed by the LockBit ransomware gang, who threatened to publish stolen data unless Boeing contacted them for ransom negotiations. The aerospace giant has made it clear that the cyber issue does not affect flight safety and is actively investigating the situation while coordinating with law enforcement and regulatory authorities.

LockBit, a Russian-linked ransomware group, claimed the cyber incident on October 27th, giving Boeing a six-day deadline to contact them. The threat actors did not specify the amount or nature of the data stolen but mentioned having a "tremendous amount." In an unusual move, LockBit refrained from providing data leak samples to protect Boeing.

Between October 30th and 31st, Boeing disappeared from LockBit's leak page, raising speculation that negotiations might be ongoing. There is no information regarding a ransom demand or any payments to LockBit.

The timing of the attack is intriguing, especially considering recent US pledges not to engage with ransomware criminals. This incident highlights the vulnerability of all organizations to ransomware and underscores the importance of robust defenses, including system patching and anti-phishing tools.

LockBit claimed a breach using a zero-day exploit but provided no additional attack details. The early announcement of cyberattacks by hacking groups remains a concern, as organizations need to quickly understand the exploited vulnerabilities for protection.

LockBit has a history of victimizing numerous organizations, with over 1,400 reported attacks worldwide. The ransomware variant LockBit 3.0 shares similarities with other Russian-linked ransomware. The group is known to have collected substantial ransom payments in Bitcoin.

Recent security reports suggest that LockBit may be experiencing management problems, resulting in an over-reliance on empty threats and a fierce reputation rather than taking substantive actions against victims.

This incident underscores the persistent threat of ransomware and the need for organizations to bolster their cybersecurity measures and rapidly respond to security incidents. Boeing's response and the ongoing investigation will be closely watched given the company's global prominence.

The source is available on the following link:

https://cybernews.com/news/boeing-confirms-cyber-attack-lockbit-ransom/

Hackers Hijack Industrial Control System at US Water Utility

The Municipal Water Authority of Aliquippa in Pennsylvania, USA, experienced a cyber-attack on a system associated with a booster station. Despite the breach, the water supply is reported to be unaffected. The compromised system, linked to a booster station overseeing water pressure for specific townships, triggered an alarm, prompting a quick response to disable the compromised system. The intrusion is attributed to a hacktivist group named Cyber Av3ngers, reportedly linked to Iran. They claim responsibility for the attack, targeting an industrial control system (ICS) manufactured by the Israeli company Unitronics. The compromised system appears to be a Unitronics Vision system, a programmable logic controller (PLC) with a human-machine interface (HMI), known for vulnerabilities.

The hacktivist group alleges breaching multiple water treatment stations in Israel, particularly since the Israel-Hamas conflict escalated on October 7. While the impact of their attacks is sometimes exaggerated, these groups target ICS to draw attention to their cause. In this case, HMIs are often left exposed to the internet without authentication, making them susceptible targets. Despite potential exaggerations, experts caution against dismissing hacktivist claims. The incident at Aliquippa water utility has been reported to the Pennsylvania State Police, but it's unclear if federal authorities are involved in the investigation. Cyberattacks on the water sector are not uncommon, leading the US government agency CISA to provide a free vulnerability scanning service for organizations in this sector.

The source is available on the following link:

https://www.securityweek.com/hackers-hijack-industrial-control-system-at-us-water-utility/

Book recommendation

Industrial Network Security

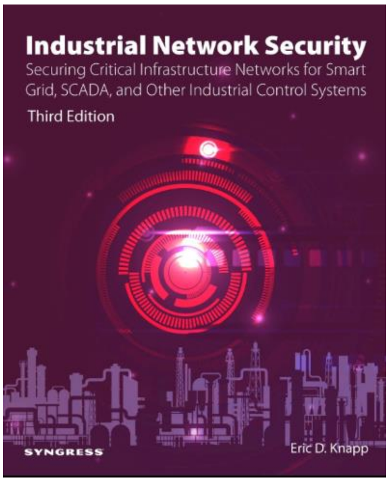
As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—becomes more important, and heavily mandated. Industrial Network Security, Third Edition arms you with the knowledge you need to understand the vulnerabilities of these distributed supervisory and control systems. Authors Eric Knapp and Joel Langill examine the unique protocols and applications that are the foundation of Industrial Control Systems (ICS) and provide clear guidelines for their protection. This comprehensive reference gives you thorough understanding of the challenges facing critical infrastructures, new guidelines and security measures for infrastructure protection, knowledge of new and evolving security tools, and pointers on SCADA protocols and security implementation. All-new real-world examples of attacks against control systems such as Trisys, Pipedream, and more diagrams of systems Includes all-new chapters on USB security and OT Cyber Kill Chains, including the lifecycle of an incident response from detection to recovery Expanded coverage of network anomaly detection and Beachhead systems for extensive monitoring and detection. New coverage of network spans, mirrors, and taps, as well as asset discovery, log collection, and industrial-focused SIEM solution

Author/Editor: Eric D. Knapp

Year of issue: **2024 March**

The book is available at the following link:

https://www.libristo.hu/hu/konyv/industrial-network-security_43723645?gclid=EAIaIQobChMIl4iZktqlggMVYpRoCR0ccAM1EAQYCCABEgJwEPD_BwE


Industrial Network Security
Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems
Third Edition
SYNGRESS
Eric D. Knapp

ICS security news selection

OT cyber attacks proliferating despite growing cybersecurity spend

The sharp increase in attacks on operational technology (OT) systems can be primarily attributed to two key factors: the escalating global threats posed by nation-state actors and the active involvement of profit-driven cybercriminals (often sponsored by the former).

The lack of success on the defense side can be attributed to several factors: the complexity of OT environments, the convergence of information technology (IT) and OT, insider attacks, supply chain vulnerabilities, and others.

Despite increased cybersecurity awareness, effort, and spending on the part of manufacturers and critical infrastructure organizations, one common misstep can help cybercriminals gain access: the insistence on visibility and detection without prevention. …

Source and more information:

https://www.helpnetsecurity.com/2023/10/26/cyber-physical-systems-cps/

New Project Analyzes and Catalogs Vendor Support for Secure PLC Coding

The new project was presented on Tuesday at SecurityWeek’s ICS Cybersecurity Conference in Atlanta by David Formby, CEO and CTO of Fortiphyd Logic, a company that specializes in endpoint detection for programmable logic controllers (PLCs) and virtual industrial control systems (ICS) security training labs.

The project builds on the ‘Top 20 Secure PLC Coding Practices’, whose goal is to provide PLC programmers with guidelines for improving security.

Some of these practices apply to all PLCs, regardless of vendor. This includes modularizing code, leaving operational logic directly in the PLC, assigning registers by function, using correlation and input plausibility checks, monitoring PLC uptime, trapping false negatives/positives, restricting third-party data interfaces, defining a safe start state in case of a restart, and validating timers, paired input/output, and indirections. …

Source and more information:

https://www.securityweek.com/new-project-analyzes-and-catalogs-vendor-support-for-secure-plc-coding/

Free Tool Helps Industrial Organizations Find OPC UA Vulnerabilities

A free tool helps industrial organizations find OPC UA (Open Platform Communications United Architecture) misconfigurations and vulnerabilities that could expose them to cyberattacks.

OPC UA is a machine-to-machine communication protocol that is used by many industrial solutions providers to ensure interoperability between various types of industrial control systems (ICS). While the protocol is highly useful, it can also pose a serious risk to organizations.

The new tool, named OpalOPC, was developed by Finland-based cybersecurity and data privacy company Molemmat Oy. …

Source and more information:

https://www.securityweek.com/free-tool-helps-industrial-organizations-find-opc-ua-vulnerabilities/

Russian Hackers Used Novel OT Attack to Disrupt Ukrainian Power Amid Mass Missile Strikes

Threat hunters at Mandiant are shining the spotlight on a pair of previously undocumented operational technology (OT) attacks last October by Russia’s “Sandworm” hackers that caused an unplanned power outage and coincided with mass missile strikes on critical infrastructure across Ukraine.

The attacks, which spanned several months and culminated in two disruptive events on October 10 and 12 last year, leveraged what Mandiant is describing as a “novel technique” for impacting industrial control systems (ICS) and OT.

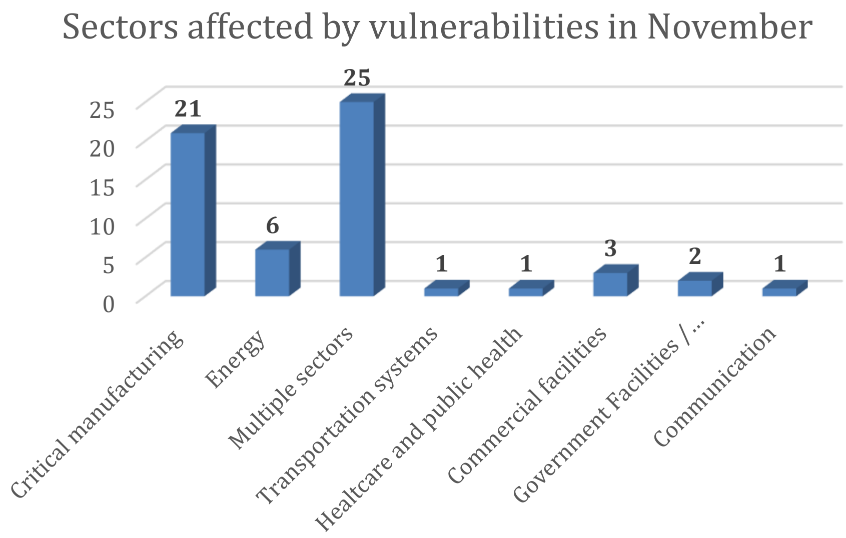
Mandiant said it caught Sandworm executing code within an end-of-life MicroSCADA control system and issuing commands that impacted the victim’s connected substations. …

Source and more information:

https://www.securityweek.com/russias-sandworm-hackers-demonstrate-lethal-ot-hacking-techniques-in-ukraine/

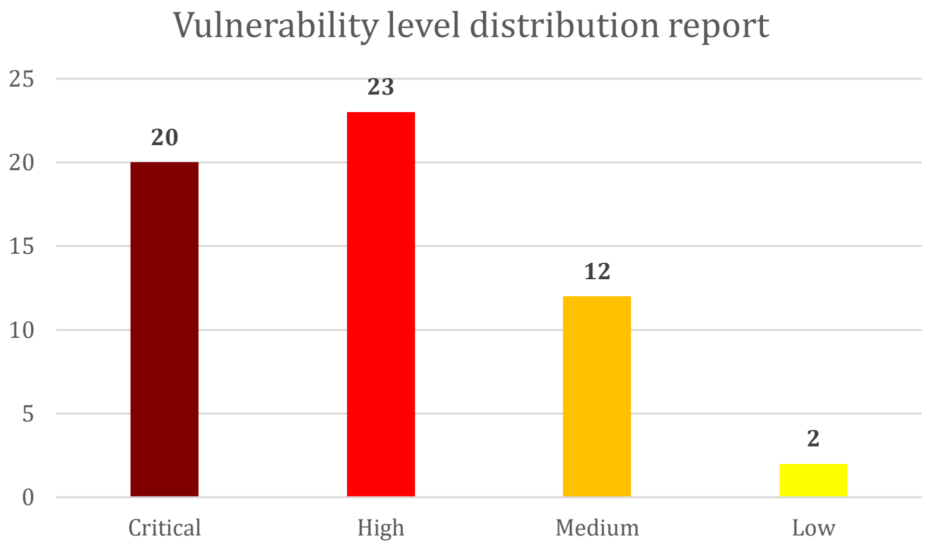
ICS vulnerabilities

In November 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 November:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	8
Out-of-bounds Write	CWE-787	6
Classic Buffer Overflow	CWE.120	4
NULL Pointer Dereference	CWE-476	4
Uncontrolled Resource Consumption	CWE-400	4



ICSA-23-334-01: **Delta Electronics DOPSoft**

High level vulnerability: Stack-Based Buffer Overflow.

Delta Electronics DOPSoft | CISA

ICSA-23-334-02: **Yokogawa STARDOM**

Medium level vulnerability: Uncontrolled Resource Consumption.

Yokogawa STARDOM | CISA

ICSA-23-334-03: **PTC KEPServerEx**

Critical level vulnerabilities: Heap-based Buffer Overflow, Improper Validation of Certificate with Host Mismatch.

PTC KEPServerEx | CISA

ICSA-23-334-04: **Mitsubishi Electric FA Engineering Software Products**

High level vulnerability: External Control of File Name or Path.

Mitsubishi Electric FA Engineering Software Products | CISA

ICSA-23-331-01: **Delta Electronics InfraSuite Device Master**

Critical level vulnerabilities: Path Traversal, Deserialization of Untrusted Data, Exposed Dangerous Method or Function.

Delta Electronics InfraSuite Device Master | CISA

ICSA-23-331-02: **Franklin Electric Fueling Systems Colibri**

Medium level vulnerability: Path Traversal.

Franklin Electric Fueling Systems Colibri | CISA

ICSA-23-331-03: **Mitsubishi Electric GX Works2**

Low level vulnerability: Denial-of-Service.

Mitsubishi Electric GX Works2 | CISA

ICSMA-23-331-01: **BD FACSChorus**

Medium level vulnerabilities: Missing Protection Mechanism for Alternate Hardware Interface, Missing Authentication for Critical Function, Improper Authentication, Use of Hard-coded Credentials, Insecure Inherited Permissions.

BD FACSChorus | CISA

ICSA-23-325-01: **WAGO PFC200 Series**

Low level vulnerability: Externally Controlled Reference to a Resource in Another Sphere.

WAGO PFC200 Series | CISA

ICSA-23-325-02: **Fuji Electric Tellus Lite V-Simulator**

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

Fuji Electric Tellus Lite V-Simulator | CISA

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

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric CNC Series (Update C) | CISA

ICSA-23-115-01: **Keysight N8844A Data Analytics Web Service (Update A)**

Critical level vulnerability: Deserialization of Untrusted Data.

Keysight N8844A Data Analytics Web Service (Update A) | CISA

ICSA-23-297-01: **Rockwell Automation Stratix 5800 and Stratix 5200 (Update A)**

Critical level vulnerabilities: Unprotected Alternate Channel, OS Command Injection.

Rockwell Automation Stratix 5800 and Stratix 5200 (Update A) | CISA

SSA-981975: **Siemens SIMATIC IPCs (Update: 1.1.)**

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

SSA-981975 (siemens.com)

SSA-975766: **Siemens Solid Edge** **(Update: 1.1.)**

High level vulnerability: Use After Free.

SSA-975766 (siemens.com)

SSA-908185: **Siemens RUGGEDCOM ROS Devices** **(Update: 1.1.)**

Critical level vulnerability: Incorrect Provision of Specified Functionality.

SSA-908185 (siemens.com)

SSA-840800: **Siemens RUGGEDCOM ROS** **(Update: 1.4.)**

High level vulnerability: Improper Control of Generation of Code ('Code Injection').

SSA-840800 (siemens.com)

SSA-831302: **Siemens SIMATIC S7-1500 TM MFP V1.0** **(Update: 1.2.)**

Critical level vulnerabilities: Multiple.

SSA-831302 (siemens.com)

SSA-794697: **Siemens SIMATIC S7-1500 TM MFP V1.0** **(Update: 1.4.)**

Critical level vulnerabilities: Multiple.

SSA-794697 (siemens.com)

SSA-787941: **Siemens RUGGEDCOM ROS devices** **(Update: 1.4.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-787941 (siemens.com)

SSA-770902: **Siemens Web Server of RUGGEDCOM ROS Devices** **(Update: 1.1.)**

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

SSA-770902 (siemens.com)

SSA-764417: **Siemens RUGGEDCOM ROS Devices** **(Update: 1.8.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-764417 (siemens.com)

SSA-711309: **Siemens SIMATIC Products** **(Update: 1.2.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-691715: **Siemens Products (Update: 1.3.)**

High level vulnerability: Improper Input Validation.

SSA-691715 (siemens.com)

SSA-647455: **Siemens RUGGEDCOM A0PE1808 devices (Update: 1.1.)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Input Validation, Incorrect Authorization, Session Fixation.

SSA-647455 (siemens.com)

SSB-439005: **Siemens SIMATIC S7-1500 CPU (Update: 5.7.)**

Critical level vulnerabilities: Multiple.

SSB-439005 (siemens.com)

SSA-407785: **Siemens Parasolid and Teamcenter Visualization (Update: 1.1.)**

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

SSA-407785 (siemens.com)

SSA-363107: **Siemens SIMATIC WinCC Kiosk Mode (Update: 1.4.)**

High level vulnerability: Insecure Default Initialization of Resource.

SSA-363107 (siemens.com)

SSA-309571: **Siemens Industrial Products using Intel CPUs (Update: 1.9.)**

High level vulnerability: Missing Encryption of Sensitive Data.

SSA-309571 (siemens.com)

SSA-306654: **Siemens Industrial Products (Update: 1.8.)**

High level vulnerabilities: multiple.

SSA-306654 (siemens.com)

SSA-264814: **Siemens SIMATIC Products (Update: 1.2.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-264814 (siemens.com)

ICSA-23-320-01: **Red Lion Sixnet RTUs**

Critical level vulnerabilities: Authentication Bypass using an Alternative Path or Channel, Exposed Dangerous Method or Function.

Red Lion Sixnet RTUs | CISA

ICSA-23-320-02: **Hitachi Energy MACH System Software**

Medium level vulnerabilities: Path Traversal, Exposure of Resource to Wrong Sphere.

Hitachi Energy MACH System Software | CISA

ICSA-23-320-03: **Siemens Desigo CC product family**

Critical level vulnerabilities: Buffer Over-Read, Heap-Based Buffer Overflow.

Siemens Desigo CC product family | CISA

ICSA-23-320-04: **Siemens Mendix Runtime**

Medium level vulnerability: Authentication Bypass by Capture-Replay.

Siemens Mendix Runtime | CISA

ICSA-23-320-05: **Siemens SCALANCE W700**

High level vulnerability: Improper Input Validation.

Siemens SCALANCE W700 | CISA

ICSA-23-320-06: **Siemens SIMATIC PCS neo**

High level vulnerabilities: Missing Authentication for Critical Function, SQL Injection, Permissive Cross-domain Policy with Untrusted Domains, Cross-site Scripting.

Siemens SIMATIC PCS neo | CISA

ICSA-23-320-07: **Siemens OPC UA Modeling Editor (SiOME)**

High level vulnerability: Improper Restriction of XML External Entity Reference.

Siemens OPC UA Modeling Editor (SiOME) | CISA

ICSA-23-320-08: **Siemens SCALANCE Family Products**

Critical level vulnerabilities: Out-of-bounds Read, Inadequate Encryption Strength, Double Free, NULL Pointer Dereference, Allocation of Resources Without Limits or Throttling, Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Hard-coded Cryptographic Key, Use of Weak Hash, Direct Request ('Forced

Browsing'), Uncontrolled Resource Consumption, Unchecked Return Value, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Unsynchronized Access to Shared Data in a Multithreaded Context.

Siemens SCALANCE Family Products | CISA

ICSA-23-320-09: **Siemens COMOS**

Critical level vulnerabilities: Improper Restriction of XML External Entity Reference, Path Traversal, Out-of-bounds Write, Out-of-bounds Read, Integer Overflow or Wraparound, Use After Free, Heap-based Buffer Overflow, Cleartext Transmission of Sensitive Information, Classic Buffer Overflow, Improper Access Control.

Siemens COMOS | CISA

ICSA-23-320-10: **Siemens SIPROTEC 4 7SJ66**

Critical level vulnerabilities: Classic Buffer Overflow, Session Fixation, NULL Pointer Dereference, Origin Validation Error, Race Condition, Missing Release of Memory after Effective Lifetime.

Siemens SIPROTEC 4 7SJ66 | CISA

ICSA-23-320-11: **Siemens Mendix Studio Pro**

High level vulnerability: Out-of-bounds Write.

Siemens Mendix Studio Pro | CISA

ICSA-23-320-12: **Siemens PNI**

Critical level vulnerabilities: Improper Input Validation, Out-of-bounds Write.

Siemens PNI | CISA

ICSA-23-320-13: **Siemens SIMATIC MV500**

Critical level vulnerabilities: Classic Buffer Overflow, NULL Pointer Dereference, Improper Authentication, Inefficient Regular Expression Complexity, Excessive Iteration, Out-of-bounds Write.

Siemens SIMATIC MV500 | CISA

ICSA-23-320-14: **Siemens RUGGEDCOM APE1808 Devices**

High level vulnerabilities: SQL Injection, Improper Input Validation.

Siemens RUGGEDCOM APE1808 Devices | CISA

ICSA-23-318-01: **AVEVA Operations Control Logger**

High level vulnerabilities: Execution with Unnecessary Privileges, External Control of File Name or Path.

AVEVA Operations Control Logger | CISA

ICSA-23-318-02: **Rockwell Automation SIS Workstation and ISaGRAF Workbench**

High level vulnerability: Improper Input Validation.

Rockwell Automation SIS Workstation and ISaGRAF Workbench | CISA

ICSA-23-313-01: **Johnson Controls Quantum HD Unity**

Critical level vulnerability: Active Debug Code.

Johnson Controls Quantum HD Unity | CISA

ICSA-23-313-02: **Hitachi Energy eSOMS**

Medium level vulnerabilities: Generation of Error Message Containing Sensitive Information, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

Hitachi Energy eSOMS | CISA

ICSA-21-334-02: **Mitsubishi Electric MELSEC and MELIPC Series (Update G)**

High level vulnerabilities: Uncontrolled Resource Consumption, Improper Handling of Length Parameter Inconsistency, Improper Input Validation.

Mitsubishi Electric MELSEC and MELIPC Series (Update G) | CISA

ICSA-23-311-01: **GE MiCOM S1 Agile**

Medium level vulnerability: Uncontrolled Search Path Element.

GE MiCOM S1 Agile | CISA

ICSA-23-306-01: **Red Lion Crimson**

High level vulnerability: Improper Neutralization of Null Byte or NUL Character.

Red Lion Crimson | CISA

ICSA-23-306-02: **Mitsubishi Electric MELSEC iQ-F Series CPU Module**

Medium level vulnerability: Improper Restriction of Excessive Authentication Attempts.

Mitsubishi Electric MELSEC iQ-F Series CPU Module | CISA

ICSA-23-306-03: **Mitsubishi Electric MELSEC Series**

Critical level vulnerability: Insufficient Verification of Data Authenticity.

Mitsubishi Electric MELSEC Series | CISA

ICSA-23-306-04: **Franklin Fueling System TS-550**

High level vulnerability: Use of Password Hash with Insufficient Computational Effort.

Franklin Fueling System TS-550 | CISA

ICSA-23-306-05: **Weintek EasyBuilder Pro**

Critical level vulnerability: Use of Hard-coded Credentials.

Weintek EasyBuilder Pro | CISA

ICSA-23-306-06: **Schneider Electric SpaceLogic C-Bus Toolkit**

Critical level vulnerabilities: Improper Privilege Management, Path Traversal.

Schneider Electric SpaceLogic C-Bus Toolkit | 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 November:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-46604 Apache ActiveMQ Deserialization of Untrusted Data Vulnerability;
CVE-2023-22518 Atlassian Confluence Data Center and Server Improper Authorization Vulnerability;
CVE-2023-29552 Service Location Protocol (SLP) Denial-of-Service Vulnerability;
CVE-2023-47246 SysAid Server Path Traversal Vulnerability;
CVE-2023-36844 Juniper Junos OS EX Series PHP External Variable Modification Vulnerability;
CVE-2023-36845 Juniper Junos OS EX Series and SRX Series PHP External Variable Modification Vulnerability;
CVE-2023-36846 Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability;
CVE-2023-36847 Juniper Junos OS EX Series Missing Authentication for Critical Function Vulnerability;
CVE-2023-36851 Juniper Junos OS SRX Series Missing Authentication for Critical Function Vulnerability;
CVE-2023-36033 Microsoft Windows Desktop Window Manager (DWM) Core Library Privilege Escalation Vulnerability;
CVE-2023-36025 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability;
CVE-2023-36036 Microsoft Windows Cloud Files Mini Filter Driver Privilege Escalation Vulnerability;
CVE-2023-36584 Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability;
CVE-2023-1671 Sophos Web Appliance Command Injection Vulnerability;
CVE-2020-2551 Oracle Fusion Middleware Unspecified Vulnerability;
CVE-2023-4911 GNU C Library Buffer Overflow Vulnerability;
CVE-2023-6345 Google Skia Integer Overflow Vulnerability;
CVE-2023-49103 ownCloud graphapi Information Disclosure Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Six Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA 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).

Links and more information:
CISA Updates Guidance for Addressing Cisco IOS XE Web UI Vulnerabilities | CISA

Atlassian Releases Security Advisory for Confluence Data Center and Server

Atlassian released a security advisory to address a vulnerability (CVE-2023-22518) affecting Confluence Data Center and Server. A cyber actor could exploit this vulnerability to obtain sensitive information.

Links and more information:
Atlassian Releases Security Advisory for Confluence Data Center and Server | CISA

Cisco Releases Security Advisories for Multiple Products

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

Links and more information:
Cisco Releases Security Advisories for Multiple Products | CISA

CISA Published When to Issue VEX Information

CISA published When to Issue Vulnerability Exploitability eXchange (VEX) Information, developed by a community of industry and government experts with the goal to offer some guidance and structure for the software security world, including the large and growing global SBOM community.

Links and more information:
CISA Published When to Issue VEX Information | CISA

FEMA and CISA Release Joint Guidance on Planning Considerations for Cyber Incidents

Federal Emergency Management Agency (FEMA) and the Cybersecurity and Infrastructure Security Agency (CISA) released the joint guide Planning Considerations for Cyber Incidents: Guidance for Emergency Managers to provide state, local, tribal, and territorial (SLTT) emergency managers with foundational knowledge of cyber incidents to increase cyber preparedness efforts in their jurisdictions.

Links and more information:

FEMA and CISA Release Joint Guidance on Planning Considerations for Cyber Incidents | CISA

CISA Releases Guidance for Addressing Citrix NetScaler ADC and Gateway Vulnerability CVE-2023-4966, Citrix Bleed

CISA, in response to active, targeted exploitation, released guidance for addressing Citrix NetScaler ADC and Gateway vulnerability CVE-2023-4966.

Links and more information:

CISA Releases Guidance for Addressing Citrix NetScaler ADC and Gateway Vulnerability CVE-2023-4966, Citrix Bleed | CISA

CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain

CISA, the National Security Agency (NSA), and partners released Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption.

Links and more information:

CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain | CISA

ACSC and CISA Release Business Continuity in a Boksz

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and CISA released Business Continuity in a Box. Business Continuity in a Box, developed by ACSC with contributions from CISA, assists organizations with swiftly and securely standing up critical business functions during or following a cyber incident.

Links and more information:

ACSC and CISA Release Business Continuity in a Box | CISA

CISA Releases Update to Royal Ransomware Advisory

Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released an update to joint Cybersecurity Advisory (CSA) #StopRansomware: Royal Ransomware.

Links and more information:

CISA Releases Update to Royal Ransomware Advisory | CISA

CISA Releases Roadmap for Artificial Intelligence Adoption

CISA released its Roadmap for Artificial Intelligence—in alignment with White House Executive Order 14110: Safe, Secure, And Trustworthy Development and Use of Artificial Intelligence—to outline a comprehensive set of actions.

Links and more information:

CISA Releases Roadmap for Artificial Intelligence Adoption | CISA

Adobe Releases Security Updates for Multiple Products

Adobe has released security updates to address vulnerabilities affecting multiple Adobe products. A cyber threat actor could exploit some of these vulnerabilities to take control of affected system.

Links and more information:

Adobe Releases Security Updates for Multiple Products | CISA

Microsoft Releases October 2023 Security Updates

Microsoft has released updates addressing multiple vulnerabilities in Microsoft software. A cyber threat actor can exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Microsoft Releases October 2023 Security Updates | CISA

Fortinet Releases Security Updates for FortiClient and FortiGate

Fortinet has released security advisories addressing vulnerabilities in FortiClient and FortiGate. Cyber threat actors may exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Fortinet Releases Security Updates for FortiClient and FortiGate | CISA

VMware Releases Security Update for Cloud Director Appliance

VMware has released a security advisory addressing a vulnerability in VMWare Cloud Director Appliance. Cyber threat actors may exploit this vulnerability to take control of an affected system.

Links and more information:

VMware Releases Security Update for Cloud Director Appliance | CISA

CISA, FBI, and MS-ISAC Release Advisory on Rhysida Ransomware

Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Rhysida Ransomware, to disseminate known Rhysida ransomware indicators of compromise (IOCs), detection methods, and tactics, techniques, and procedures (TTPs) identified through investigations as recently as September 2023.

Links and more information:

CISA, FBI, and MS-ISAC Release Advisory on Rhysida Ransomware | CISA

FBI and CISA Release Advisory on Scattered Spider Group

Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA) on Scattered Spider—a cybercriminal group targeting commercial facilities sectors and subsectors. The advisory provides tactics, techniques, and procedures (TTPs) obtained through FBI investigations as recently as November 2023.

Links and more information:

FBI and CISA Release Advisory on Scattered Spider Group | CISA

Citrix Releases Security Updates for Citrix Hypervisor

Citrix has released security updates addressing vulnerabilities in Citrix Hypervisor 8.2 CU1 LTSR. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.

Links and more information:

Citrix Releases Security Updates for Citrix Hypervisor | CISA

CISA Releases The Mitigation Guide: Healthcare and Public Health (HPH) Sector

CISA released the Mitigation Guide: Healthcare and Public Health (HPH) Sector as a supplemental companion to the HPH Cyber Risk Summary, published July 19, 2023. This guide provides defensive mitigation strategy recommendations and best practices to combat pervasive cyber threats affecting this critical infrastructure sector.

Links and more information:

CISA Releases The Mitigation Guide: Healthcare and Public Health (HPH) Sector | CISA

Juniper Releases Security Advisory for Juniper Secure Analytics

Juniper released a security advisory to address multiple vulnerabilities affecting Juniper Secure Analytics. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Juniper Releases Security Advisory for Juniper Secure Analytics | CISA

CISA, FBI, MS-ISAC, and ASD's ACSC Release Advisory on LockBit Affiliates Exploiting Citrix Bleed

Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Multi-State Information Sharing & Analysis Center (MS-ISAC), and Australian Signals Directorate's Australian Cyber Security Center (ASD's ACSC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: LockBit Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability.

Links and more information:

CISA, FBI, MS-ISAC, and ASD's ACSC Release Advisory on LockBit Affiliates Exploiting Citrix Bleed | CISA

Mozilla Releases Security Updates for Firefox and Thunderbird

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

Links and more information:

Mozilla Releases Security Updates for Firefox and Thunderbird | CISA

Adobe Releases Security Updates for ColdFusion

Adobe released security updates addressing vulnerabilities affecting unpatched ColdFusion software. Exploitation of some of these vulnerabilities may allow a malicious cyber actor to take control of an affected system.

Links and more information:

Adobe Releases Security Updates for ColdFusion | CISA

CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development

U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) are proud to announce the release of the Guidelines for Secure AI System Development.

Links and more information:

CISA and UK NCSC Unveil Joint Guidelines for Secure AI System Development | CISA

Exploitation of Unitronics PLCs used in Water and Wastewater Systems

CISA is responding to active exploitation of Unitronics programmable logic controllers (PLCs) used in the Water and Wastewater Systems (WWS) Sector.

Links and more information:

Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA

CISA Releases First Secure by Design Alert

CISA published guidance on How Software Manufacturers Can Shield Web Management Interfaces From Malicious Cyber Activity as a part of a new Secure by Design (SbD) Alert series.

Links and more information:

CISA Releases First Secure by Design Alert | CISA