2023 September, 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

Top 5 ICS Security Best Practices

Industrial organizations face an increasing array of cyber threats, from ransomware campaigns to nation-state attacks. To safeguard operations against these growing threats, it's crucial to implement the following core cybersecurity practices in operational technology (OT) environments:

1. Comprehensive Device Understanding: Begin with a thorough inventory of all devices in your industrial control systems (ICS). This goes beyond hardware and software, encompassing physical location, significance to industrial processes, and contact information for issue resolution. Traditional IT inventory methods are often inadequate for ICS, and passive network monitoring, alongside other techniques, can provide a more complete picture of your systems.
2. Centralized User Account Management: Many ICS systems use standard usernames and passwords, which can pose security risks. Centralized monitoring and management of user accounts, access, authentication, and account changes are essential. Implement policies that enforce complex passwords and restrict access based on necessity.
3. Automated Vulnerability Monitoring: As critical vulnerabilities are discovered more frequently, a vulnerability-first approach is essential. Automate the identification of vulnerabilities by comparing ICS device data with databases like NIST's CVE and ICS-CERT advisories. Prioritize patching and mitigation efforts based on this information.
4. Suspicious Change Detection: Continuously monitor configurations of endpoints to detect any unauthorized changes. Be vigilant about removable media, which can be an attack vector. Utilize network intrusion detection systems to identify communication anomalies and complement endpoint monitoring for robust threat detection.
5. Empower Security Responders: Ensure that your security team understands ICS environments and has access to actionable data. Cross-training between IT and OT teams is valuable. Invest in specialized ICS cybersecurity solutions that provide relevant data on asset importance, location, and contacts, and ensure seamless integration with corporate security systems.

To maintain critical security practices, rely on automated methods to identify, monitor, and manage assets and document changes comprehensively.

Manual approaches like spreadsheets are prone to errors and outdated information. It's crucial to adopt OT-specific cybersecurity measures that align with operational goals while recognizing that IT and OT environments have unique requirements. Collaboration between IT and OT security teams is vital to protect critical infrastructure effectively.

Source and more information available on the following link:

https://www.industrialdefender.com/blog/top-5-ics-security-best-practices

ICS trainings, education

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

ICS conferences

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

International Conference on Industrial Control Systems Security

International Conference on Industrial Control Systems Security aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Industrial Control Systems Security. This ICS Cyber Security Conference 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 Industrial Control Systems Security.

Tbilisi, Georgia; 04th – 05th October 2023

More details can be found on the following website:

https://www.upcomingengineeringconferences.com/international-conference-on-industrial-control-systems-security.html

GridSecCon 2023

NERC, the E-ISAC, and Northeast Power Coordinating Council (NPCC) are co-hosting the 12th annual grid security conference on October 18 – 20 with training opportunities on October 17 in Québec City, Canada. GridSecCon brings together cyber and physical security leaders from industry and government to deliver expert training sessions, share best practices and effective threat mitigation programs, and present lessons learned.

Québec City, Canada; 18th – 20th October 2023

More details can be found on the following website:

https://www.nerc.com/pa/CI/ESISAC/Pages/GridSecCon.aspx

Industrial Control Systems (ICS) Cyber Security Conference

SecurityWeek's ICS Cyber Security Conference is the conference where ICS users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyze their causes and cooperate on solutions. Since its first edition in 2002, the conference has attracted a continually rising interest as both the stakes of critical infrastructure protection and the distinctiveness of securing ICSs become increasingly apparent.

Atlanta GA, USA; 23rd – 26th October 2023

More details can be found on the following website:

https://www.icscybersecurityconference.com/

EnergySec Internal Controls/Supply Chain Security - Portland, OR [HYBRID]

This course will provide an understanding of security control frameworks and the application of internal controls in NERC CIP environments. It will cover the NIST SP800 series controls, NIST CSF, ES-C2M2, and related mappings to the standards. The target audience is compliance professionals, technical SMEs, management, and others that desire a deeper understanding of controls.

This course will also provide an understanding of supply chain security risks relevant in the electric sector and mitigation strategies. The CIP supply chain standards will be covered in detail as well as Presidential Executive Orders, NERC Supply Chain Risk Mitigation Program documents, and more.

Portland Southeast/Clackamas, OR, USA; 24th – 26th October 2023

More details can be found on the following website:

https://events.eventzilla.net/e/energysec-internal-controlssupply-chain-security--portland-or-hybrid-2138619032?resp=on&dateid=2138419368

ICS incidents

Cyberattack on Ukrainian Critical Energy Infrastructure

The Computer Emergency Response Team of Ukraine (CERT-UA) announced its successful thwarting of a cyber attack against a critical energy infrastructure facility in Ukraine. The attack, which was attributed to the Russian threat actor APT28, began with a phishing email containing a link to a malicious ZIP archive, initiating the infection process.

When the victim clicked on the link, it triggered the download of a ZIP archive containing three JPG images as decoys and a BAT file named 'weblinks.cmd' onto the victim's computer. Running the CMD file resulted in the opening of several decoy web pages, the creation of .bat and .vbs files, and the execution of a VBS file, which, in turn, executed the BAT file.

In the next phase of the attack, the "whoami" command was run on the compromised host, and the gathered information was exfiltrated. Additionally, the attacker downloaded the TOR hidden service to route malicious traffic. Persistence was established through a scheduled task, and remote command execution was achieved using cURL, which utilized a legitimate service called webhook.site. It's important to note that this service had been recently disclosed as being used by a threat actor known as Dark Pink.

Fortunately, the attack was ultimately unsuccessful because access to Mocky and the Windows Script Host (wscript.exe) had been restricted. APT28 had previously been associated with the use of Mocky APIs. This disclosure comes amidst a series of phishing attacks targeting Ukraine, with some of them employing an off-the-shelf malware obfuscation engine called ScruptCrypt to distribute AsyncRAT.

Furthermore, another cyber assault attributed to GhostWriter (also known as UAC-0057 or UNC1151) was reported to have weaponized a recently disclosed zero-day vulnerability in WinRAR (CVE-2023-38831, CVSS score: 7.8) to deploy PicassoLoader and Cobalt Strike, according to CERT-UA.

The source is available on the following link:

https://thehackernews.com/2023/09/ukraines-cert-thwarts-apt28s.html

Book recommendation

Cyber Security Operational Technology Best Practice

Cyber Operational Technology (OT) refers to the systems and devices that are used to control and monitor physical processes in industries such as manufacturing, power generation, and transportation. These systems are often connected to the internet, making them vulnerable to cyber attacks.

OT systems are typically not designed with cybersecurity in mind and can be more difficult to secure than traditional IT systems.

You don't have to be a tech-junkie to understand the basics of cyber security, and this book will show you how easy it can be to shield yourself from attackers!

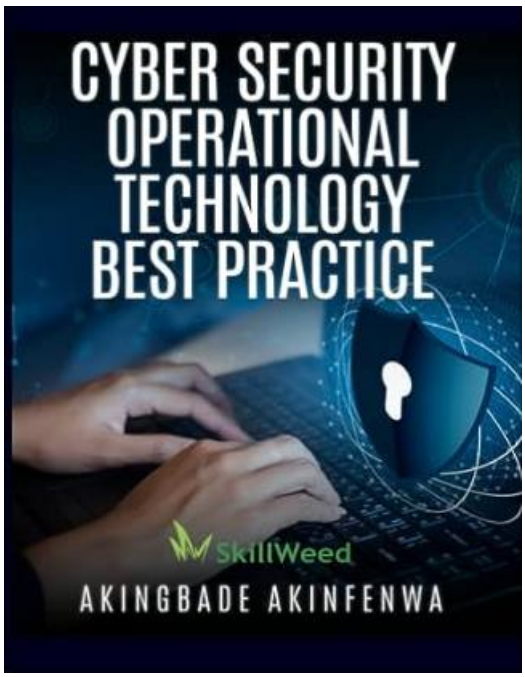
As such, the security of OT systems is becoming an increasingly important concern, as cyber attacks on these systems can have severe consequences, such as physical damage to equipment or disruption of essential services.

ICS systems are used to control industrial processes and infrastructure such as power plants, water treatment facilities, and transportation systems.

Year of issue: 2023

The book is available at the following link:

https://www.amazon.ca/CYBER-SECURITY-OPERATIONAL-TECHNOLOGY-PRACTICE/dp/1649537387



ICS security news selection

MITRE, CISA publish open-source MITRE Caldera for OT plugins, supporting common industrial protocols

Not-for-profit organization MITRE announced that its MITRE Caldera team has announced the release of Caldera for OT, a collection of Caldera plugins that provide support for common industrial protocols. These initial Caldera for OT (operational technology) extensions were developed in partnership with the Homeland Security Systems Engineering and Development Institute (HSSEDI), a federally funded research and development center that is managed and operated by MITRE for the U.S. Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA) to increase the resiliency of critical infrastructure. …

Source, and more information:

https://industrialcyber.co/critical-infrastructure/mitre-cisa-publish-open-source-mitre-caldera-for-ot-plugins-supporting-common-industrial-protocols/

QR Code Campaign Targets Major Energy Firm

A significant phishing campaign employing QR codes has recently come to light, with a major US-based energy company as one of the primary targets.

The campaign, which began in May 2023, has witnessed a 2400% surge in volume since then, underscoring the urgency of addressing this emerging threat.

Cybersecurity company Cofense has been closely monitoring this campaign. In an advisory published on Wednesday, the company said that over 29% of the malicious emails, numbering more than 1000, were directed at the energy sector giant. Other industries also fell victim, with manufacturing, insurance, technology and financial services companies accounting for a combined 37% of the attacks.

The attackers' modus operandi involves sending emails masquerading as Microsoft security notifications. These emails contain PNG or PDF attachments, enticing users to scan QR codes purportedly for enhanced security measures. …

Source, and more information:

https://www.infosecurity-magazine.com/news/qr-codes-target-energy-firm/

Rising OT/ICS cybersecurity incidents reveal alarming trend

60% of cyberattacks against the industrial sector are led by state-affiliated actors and often unintentionally enabled by internal personnel (about 33% of the time), according to Rockwell Automation.

This corroborates other industry research showing OT/ICS (Industrial Control Systems) cybersecurity incidents are increasing in volume and frequency, and are targeting critical infrastructure, such as energy producers.

Insiders unintentionally aid threat actors

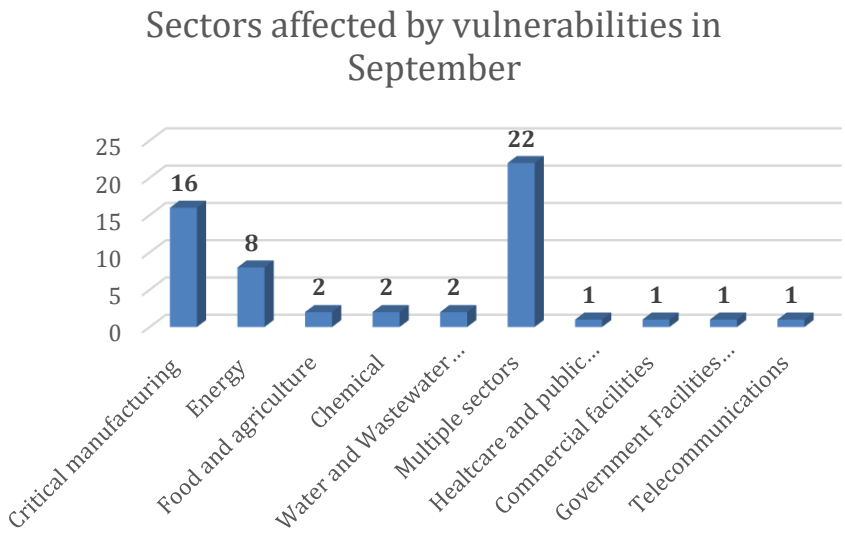
"Energy, critical manufacturing, water treatment and nuclear facilities are among the types of critical infrastructure industries under attack in the majority of reported incidents," said Mark Cristiano, commercial director of Global Cybersecurity Services at Rockwell Automation. …

Source, and more information:

https://www.helpnetsecurity.com/2023/09/20/ot-ics-cybersecurity-incidents/

ICS vulnerabilities

In September 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:

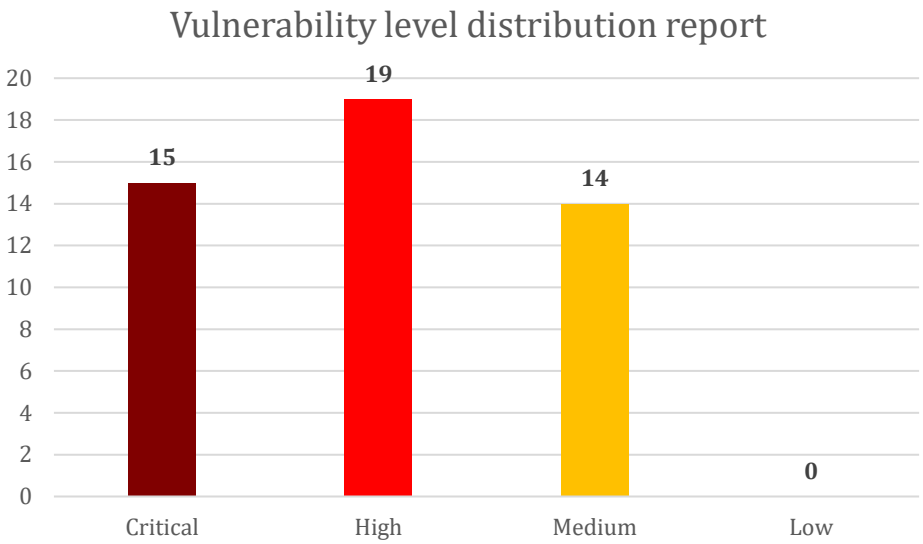


Average number of vulnerabilities per vulnerability report in September: **2,09**

Vulnerabilities/Exploitable remotely: **48/35**

The most common vulnerabilities in September:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	5
Cross-site Scripting	CWE-79	5
Out-of-bounds Write	CWE-787	5
Plaintext Storage of a Password	CWE-256	5



ICSA-23-271-01: **Rockwell Automation PanelView 800**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation PanelView 800 | CISA

ICSA-23-271-02: **DEXMA DexGate**

High level vulnerabilities: Cross-Site Scripting, Cross-Site Request Forgery, Improper Authentication, Cleartext Transmission of Sensitive Information, Exposure of Sensitive Information to an Unauthorized Actor.

DEXMA DexGate | CISA

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

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

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

ICSA-23-269-01: **Suprema BioStar 2**

Medium level vulnerability: SQL Injection.

Suprema BioStar 2 | CISA

ICSA-23-269-02: **Hitachi Energy Asset Suite 9**

Medium level vulnerability: Improper Authentication.

Hitachi Energy Asset Suite 9 | CISA

ICSA-23-269-03: **Mitsubishi Electric FA Engineering Software**

Critical level vulnerability: Incorrect Default Permissions.

Mitsubishi Electric FA Engineering Software | CISA

ICSA-23-269-04: **Advantech EKI-1524-CE series**

Medium level vulnerability: Cross-Site Scripting.

Advantech EKI-1524-CE series | CISA

ICSA-23-269-05: **Baker Hughes Bently Nevada 3500**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Cleartext Transmission of Sensitive Information, Authentication Bypass by Capture-replay.

Baker Hughes Bently Nevada 3500 | CISA

ICSA-23-024-02: **SOCOMEC MODULYS GP (UPDATE A)**

Medium level vulnerability: Weak Encoding for Password.

SOCOMEC MODULYS GP (UPDATE A) | CISA

ICSA-23-264-01: **Real Time Automation 460 Series**

Critical level vulnerability: Cross-site Scripting.

Real Time Automation 460 Series | CISA

ICSA-23-264-02: **Siemens Spectrum Power 7**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens Spectrum Power 7 | CISA

ICSA-23-264-03: **Delta Electronics DIAScreen**

High level vulnerability: Out-of-bounds Write.

Delta Electronics DIAScreen | CISA

ICSA-23-264-04: **Rockwell Automation Select Logix Communication Modules**

Critical level vulnerability: Stack-based Buffer Overflow.

Rockwell Automation Select Logix Communication Modules | CISA

ICSA-23-264-05: **Rockwell Automation Connected Components Workbench**

Critical level vulnerabilities: Use After Free, Out-of-bounds Write.

Rockwell Automation Connected Components Workbench | CISA

ICSA-23-264-06: **Rockwell Automation FactoryTalk View Machine Edition**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk View Machine Edition | CISA

ICSA-23-262-01: **Siemens SIMATIC PCS neo Administration Console**

Medium level vulnerability: Insertion of Sensitive Information into Externally-Accessible File or Directory.

Siemens SIMATIC PCS neo Administration Console | CISA

ICSA-23-262-03: **Omron Engineering Software Zip-Slip**

Medium level vulnerability: Path Traversal.

Omron Engineering Software Zip-Slip | CISA

ICSA-23-262-04: **Omron Engineering Software**

Medium level vulnerability: Improper Authorization.

Omron Engineering Software | CISA

ICSA-23-262-05: **Omron CJ/CS/CP Series**

High level vulnerability: Improper Control of Interaction Frequency.

Omron CJ/CS/CP Series | CISA

SSA-831302: **Siemens SIMATIC S7-1500 TM MFP V1.0 (Update 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-831302 (siemens.com)

SSA-794697: **Siemens SIMATIC S7-1500 TM MFP V1.0 (Update 1.3.)**

Critical level vulnerabilities: Multiple.

SSA-794697 (siemens.com)

SSA-787941: **Siemens RUGGEDCOM ROS V4 (Update 1.3.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-787941 (siemens.com)

SSA-764801: **Siemens Tecnomatix Plant Simulation (Update 1.2.)**

High level vulnerabilities: Heap-based Buffer Overflow, Out-of-bounds Write, Stack-based Buffer Overflow, Access of Resource Using Incompatible Type ('Type Confusion').

SSA-764801 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update 2.3.)**

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

SSA-712929 (siemens.com)

SSA-587547: **Siemens QMS Automotive (Update 1.1.)**

High level vulnerability: Plaintext Storage of a Password.

SSA-587547 (siemens.com)

SSA-552874: **Siemens SIPROTEC 5 Devices (Update 1.2.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-552874 (siemens.com)

SSA-478960: **Siemens Industrial Controllers (Update 1.1.)**

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

SSA-478960 (siemens.com)

SSA-450613: **Siemens RUGGEDCOM APE1808 Product Family (Update 1.1.)**

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

SSA-450613 (siemens.com)

SSA-382653: **Siemens Industrial Products (Update 1.5.)**

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-322980: **Siemens SIPROTEC 5 Devices (Update 1.2.)**

High level vulnerability: NULL Pointer Dereference.

SSA-322980 (siemens.com)

SSA-264815: **SIMATIC Products (Update 1.1.)**

High level vulnerability: Improper Input Validation.

SSA-264815 (siemens.com)

SSA-264814: **SIMATIC Products (Update 1.1.)**

Medium level vulnerability: Inadequate Encryption Strength.

SSA-264814 (siemens.com)

ICSA-23-257-01: **Siemens SIMATIC, SIPLUS Products**

High level vulnerability: Integer Overflow or Wraparound.

Siemens SIMATIC, SIPLUS Products | CISA

ICSA-23-257-02: **Siemens Parasolid**

High level vulnerability: Out-of-bounds Write.

Siemens Parasolid | CISA

ICSA-23-257-03: **Siemens QMS Automotive**

High level vulnerabilities: Plaintext Storage of a Password, Cleartext Storage of Sensitive Information in Memory, Generation of Error Message Containing Sensitive Information, Server-generated Error Message Containing Sensitive Information, Improper Verification of Cryptographic Signature, Insecure Storage of Sensitive Information, Cleartext Transmission of Sensitive Information, Improper Access Control, Unrestricted Upload of File with Dangerous Type, Insufficient Session Expiration.

Siemans QMS Automotive | CISA

ICSA-23-257-04: **Siemens RUGGEDCOM APE1808 Product**

High level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Buffer Underflow, Classic Buffer Overflow, Time-of-check Time-of-use Race Condition, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Improper Input Validation, Missing Release of Memory after Effective Lifetime, Improperly Implemented Security Check for Standard, Plaintext Storage of a Password.

Siemens RUGGEDCOM APE1808 Product Family | CISA

ICSA-23-257-05: **Siemens SIMATIC IPCs**

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

Siemens SIMATIC IPCs | CISA

ICSA-23-257-06: **Siemens WIBU Systems CodeMeter**

Critical level vulnerability: Heap-Based Buffer Overflow.

Siemans WIBU Systems CodeMeter | CISA

ICSA-23-257-07: **Rockwell Automation Pavilion8**

High level vulnerability: Improper Authentication.

Rockwell Automation Pavilion8 | CISA

ICSA-23-255-01: **Hitachi Energy Lumada APM Edge**

High level vulnerabilities: Use After Free, Double Free, Type Confusion, Observable Discrepancy.

Hitachi Energy Lumada APM Edge | CISA

ICSA-23-255-02: **Fujitsu Software Infrastructure Manager**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

Fujitsu Software Infrastructure Manager | CISA

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

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric MELSEC Series CPU module (Update) | CISA

ICSA-23-250-01: **Dover Fueling Solutions MAGLINK LX Console**

Critical level vulnerabilities: Authentication Bypass using an Alternate Path or Channel, Improper Access Control, Path Traversal.

Dover Fueling Solutions MAGLINK LX Console | CISA

ICSA-23-250-02: **Phoenix Contact TC ROUTER and TC CLOUD CLIENT**

Critical level vulnerabilities: Cross-site Scripting, XML Entity Expansion.

Phoenix Contact TC ROUTER and TC CLOUD CLIENT | CISA

ICSA-23-250-03: **Socomec MOD3GP-SY-120K**

Critical level vulnerabilities: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Storage of Sensitive Information, Reliance on Cookies without Validation and Integrity Checking, Code Injection, Plaintext Storage of a Password.

Socomec MOD3GP-SY-120K | CISA

ICSA-23-157-01: **Delta Electronics CNCSoft-B DOPSoft (Update)**

High level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow.

Delta Electronics CNCSoft-B DOPSoft (Update) | CISA

ICSA-23-248-01: **Fujitsu Limited Real-time Video Transmission Gear IP series**

Medium level vulnerability: Use Of Hard-Coded Credentials.

Fujitsu Limited Real-time Video Transmission Gear "IP series" | CISA

ICSMA-23-248-01: **Softneta MedDream PACS Premium**

Critical level vulnerabilities: Exposed Dangerous Method or Function, Plaintext Storage of a Password.

Softneta MedDream PACS | 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 September:

VMware Releases Security Update for Tools
VMware has released a security update to address a vulnerability in VMware Tools. A cyber threat actor can exploit this vulnerability to obtain sensitive information.
Link and more information:
VMware Releases Security Update for Tools | CISA

CISA Adds One Known Vulnerability to Catalog
CVE-2023-33246 Apache RocketMQ Command Execution Vulnerability;
Link and more information:
CISA Adds One Known Vulnerability to Catalog | CISA

CISA Releases Capacity Enhancement Guide to Strengthen Agency Resilience to DDoS Attack
CISA has released actionable guidance for Federal Civilian Executive Branch (FCEB) agencies to help them evaluate and mitigate the risk of volumetric distributed denial-of-service (DDoS) attacks against their websites and related web services.
Link and more information:
CISA Releases Capacity Enhancement Guide to Strengthen Agency Resilience to DDoS Attack | CISA

CISA Releases Update to Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells
The Cybersecurity and Infrastructure Security Agency (CISA) has released an update to a previously published Cybersecurity Advisory (CSA), Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells.
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/06/cisa-releases-update-threat-actors-exploiting-citrix-cve-2023-3519-implant-webshells

Cisco Releases Security Advisories for Multiple Products
CISA encourages users and administrators to review the following advisories and apply the necessary updates. BroadWorks and BroadWorks Xtended and Identity Services Engine RADIUS;
Link and more information:
Cisco Releases Security Advisories for Multiple Products | CISA

CISA, FBI, and CNMF Release Advisory on Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475

CISA, Federal Bureau of Investigation (FBI), and U.S. Cyber Command's Cyber National Mission Force (CNMF) published a joint Cybersecurity Advisory (CSA), Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475.

Link and more information:

CISA, FBI, and CNMF Release Advisory on Multiple Nation-State Threat Actors Exploit CVE-2022-47966 and CVE-2022-42475 | CISA

CISA Adds Two Known Vulnerabilities to Catalog

CVE-2023-41064 Apple iOS, iPadOS, and macOS ImageIO Buffer Overflow
CVE-2023-41061 Apple iOS, iPadOS, and watchOS Wallet Code Execution Vulnerability

Link and more information:

CISA Adds Two Known Vulnerabilities to Catalog | CISA

NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats

National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) released a Cybersecurity Information Sheet (CSI), Contextualizing Deepfake Threats to Organizations, which provides an overview of synthetic media threats, techniques, and trends.

Link and more information:

NSA, FBI, and CISA Release Cybersecurity Information Sheet on Deepfake Threats | CISA

CISA Adds Two Known Vulnerabilities to Catalog

CVE-2023-36761 Microsoft Word Information Disclosure Vulnerability
CVE-2023-36802 Microsoft Streaming Service Proxy Elevation of Privilege Vulnerability

Link and more information:

CISA Adds Two Known Vulnerabilities to Catalog | CISA

CISA Releases its Open Source Software Security Roadmap

CISA released an Open Source Software Security Roadmap to lay out—in alignment with the National Cybersecurity Strategy and the CISA Cybersecurity Strategic Plan—how we will partner with federal agencies, open source software (OSS) consumers, and the OSS community, to secure OSS infrastructure.

Link and more information:

CISA Releases its Open Source Software Security Roadmap | CISA

Adobe Releases Security Updates for Multiple Products

Adobe Connect: APSB23-33
Adobe Acrobat and Reader: APSB23-34
Adobe Experience Manager: APSB23-43

Link and more information:
Adobe Releases Security Updates for Multiple Products | CISA

Microsoft Releases September 2023 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 September 2023 Updates | CISA

Apple Releases Security Updates for iOS and macOS
CISA encourages users and administrators to review the following advisories and apply the necessary updates.
iOS 15.7.9 and iPadOS 15.7.9
macOS Monterey 12.6.9
macOS Big Sur 11.7.10
Link and more information:
Apple Releases Security Updates for iOS and macOS | CISA

CISA Adds Three Known Vulnerabilities to Catalog
CVE-2023-35674 Android Framework Privilege Escalation Vulnerability
CVE-2023-20269 Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability
CVE-2023-4863 Google Chrome Heap-Based Buffer Overflow Vulnerability
Link and more information:
CISA Adds Three Known Vulnerabilities to Catalog | CISA

Mozilla Releases Security Updates for Multiple Products
Mozilla has released security updates to address a vulnerability affecting Firefox, Firefox ESR, and Thunderbird. A cyber threat actor can exploit this vulnerability to take control of an affected system.
Link and more information:
Mozilla Releases Security Updates for Multiple Products | CISA

CISA Adds One Known Vulnerability to Catalog
CVE-2023-26369 Adobe Acrobat and Reader Out-of-Bounds Write Vulnerability;
Link and more information:
CISA Adds One Known Vulnerability to Catalog | CISA

CISA Releases Continuous Diagnostics and Mitigation Program: Identity, Credential, and Access Management (ICAM) Reference Architecture
CISA released the Continuous Diagnostics and Mitigation Program: Identity, Credential, and Access Management (ICAM) Reference Architecture to help federal civilian

departments and agencies integrate their identity and access management (IDAM) capabilities into their ICAM architectures.
Link and more information:
CISA Releases Continuous Diagnostics and Mitigation Program: Identity, Credential, and Access Management (ICAM) Reference Architecture | CISA

Fortinet Releases Security Updates for Multiple Products
Fortinet has released security updates to address vulnerabilities (CVE-2023-29183 and CVE-2023-34984) affecting FortiOS, FortiProxy, and FortiWeb. A cyber threat actor can exploit one of these vulnerabilities to take control of an affected system.
Link and more information:
Fortinet Releases Security Updates for Multiple Products | CISA

CISA Adds Eight Known Exploited Vulnerabilities to Catalog
CVE-2022-22265 Samsung Mobile Devices Use-After-Free Vulnerability
CVE-2014-8361 Realtek SDK Improper Input Validation Vulnerability
CVE-2017-6884 Zyxel EMG2926 Routers Command Injection Vulnerability
CVE-2021-3129 Laravel Ignition File Upload Vulnerability
CVE-2022-31459 Owl Labs Meeting Owl Inadequate Encryption Strength Vulnerability
CVE-2022-31461 Owl Labs Meeting Owl Missing Authentication for Critical Function Vulnerability
CVE-2022-31462 Owl Labs Meeting Owl Use of Hard-coded Credentials Vulnerability
CVE-2022-31463 Owl Labs Meeting Owl Improper Authentication Vulnerability
Link and more information:
CISA Adds Eight Known Exploited Vulnerabilities to Catalog | CISA

CISA Adds One Known Exploited Vulnerability to Catalog
CVE-2023-28434 MinIO Security Feature Bypass Vulnerability;
Link and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

FBI and CISA Release Advisory on Snatch Ransomware
Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released joint Cybersecurity Advisory (CSA) #StopRansomware: Snatch Ransomware, which provides indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) associated with the Snatch ransomware variant.
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/20/fbi-and-cisa-release-advisory-snatch-ransomware

CISA Adds One Known Exploited Vulnerability to Catalog
CVE-2023-41179 Trend Micro Apex One and Worry-Free Business Security Remote Code Execution Vulnerability;

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/21/cisa-adds-one-known-exploited-vulnerability-catalog

Drupal Releases Security Advisory to Address Vulnerability in Drupal Core
Drupal has released a security advisory to address a vulnerability affecting multiple Drupal versions. A malicious cyber actor could exploit this vulnerability to take control of an affected system.
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/21/drupal-releases-security-advisory-address-vulnerability-drupal-core

ISC Releases Security Advisories for BIND 9
The Internet Systems Consortium (ISC) has released security advisories to address vulnerabilities affecting ISC's Berkeley Internet Name Domain (BIND) 9. A malicious cyber actor could exploit these vulnerabilities to cause denial-of-service conditions.
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/21/isc-releases-security-advisories-bind-9

Atlassian Releases September Security Bulletin
Atlassian has released its security bulletin for September 2023 to address vulnerabilities in multiple products. A malicious cyber actor could exploit some of these vulnerabilities to take control of an affected system.
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/21/atlassian-releases-september-security-bulletin

Apple Releases Security Updates 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:
https://www.cisa.gov/news-events/alerts/2023/09/22/apple-releases-security-updates-multiple-products

CISA Adds Three Known Exploited Vulnerabilities to Catalog
CVE-2023-41991 Apple Multiple Products Improper Certificate Validation Vulnerability
CVE-2023-41992 Apple Multiple Products Kernel Privilege Escalation Vulnerability
CVE-2023-41993 Apple Multiple Products WebKit Code Execution Vulnerability
Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/25/cisa-adds-three-known-exploited-vulnerabilities-catalog

NSA, FBI, CISA, and Japanese Partners Release Advisory on PRC-Linked Cyber Actors

U.S. National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cybersecurity and Infrastructure Security Agency (CISA), along with the Japan National Police Agency (NPA) and the Japan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) released joint Cybersecurity Advisory (CSA) People's Republic of China-Linked Cyber Actors Hide in Router Firmware.

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/27/nsa-fbi-cisa-and-japanese-partners-release-advisory-prc-linked-cyber-actors

Mozilla Releases Security Advisories for Thunderbird and Firefox

Mozilla has released security updates to address vulnerabilities for Thunderbird 115.3, Firefox ESR 115.3, and Firefox 118. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/27/mozilla-releases-security-advisories-thunderbird-and-firefox

Apple Releases Security Updates 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 system.

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/28/apple-releases-security-updates-multiple-products

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2018-14667 Red Hat JBoss RichFaces Framework Expression Language Injection Vulnerability;

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/28/cisa-adds-one-known-exploited-vulnerability-catalog

Cisco Releases Security Advisories for Multiple Products

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

Link and more information:
https://www.cisa.gov/news-events/alerts/2023/09/28/cisco-releases-security-advisories-multiple-products