2023 August, 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

Operational Technology (OT) Security Best Practices in 2023

There is a Geekflare article, which discusses Operational Technology (OT) Security best practices in 2023, focusing on protecting production operations in automatic product manufacturing plants from cyber threats. It explains that OT is the use of software and hardware to control real-world manufacturing processes and industrial infrastructure. With the rise of the Industrial Internet of Things (IIoT), the risk of cyber threats to OT systems has increased, making OT security crucial for ensuring continuous and safe operations.

OT security involves employing various hardware and software measures to protect industrial control systems from cyber threats. It emphasizes the need for protection against cyber-attacks and the importance of business continuity. The article also provides best practices for OT security, including OT asset discovery, network segmentation, OT threat prevention, and for identity and access management, adopting a Zero-Trust framework, and monitoring for suspicious activities.

The article further explores the differences between IT and OT security, highlighting the technology and tools used in each and their exposure to cyber threats. It discusses the convergence of IT and OT networks in modern businesses and the need for robust data and systems security in this scenario.

To enhance OT security knowledge, the article suggests learning resources, such as books and courses, that cover OT cybersecurity concepts, operations, and technology solutions. It emphasizes the criticality of securing industrial control systems against cyber threats to protect production facilities from potential disruptions.

In conclusion, the article stresses the importance of implementing operational technology best practices in 2023 to safeguard production facilities from cyber threats, especially as IT and OT networks converge, creating complex security challenges.

Source and more information available on the following link:

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

ICS trainings, education

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

New in this ICS security feed:

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

Cyber Security for Critical Industries

With the rapid advancements in technology and connectivity, these attacks are becoming increasingly complex and difficult to detect. Cybersecurity, therefore, needs to be a top priority for companies seeking to identify new risks and increase their resilience to the evolving threats to critical systems.

Cyber Security for Industrial Control Systems will focus on identifying the latest cybersecurity challenges facing companies today and examine how these can be mitigated by building resilient and responsive systems.

You will also get exclusive insights into new techniques and technologies. Plus, the opportunity to network with some of the UK's cybersecurity giants makes this a must-attend conference for anyone working in critical systems.

London, UK; 12th – 13th September 2023

More details can be found on the following website:

https://industrialcyber.co/event/cyber-security-for-industrial-control-systems/

10th annual Control Systems Cybersecurity USA conference

The Cyber Senate Control Systems Cybersecurity USA 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. Case studies, roundtables and panel sessions throughout the two-day event will demonstrate how your peers have fortified their defenses; from maturing and adopting better ways to tighten network segmentation and security controls to ensuring their strategies are effective, scalable, adaptable and repeatable in the face of evolving cyber threats. Not only will we be reinforcing winning formulas from the OT security playbook, we will help practitioners translate the plays and help them remove the complexity of staying in the game.

Nashville TN, USA; 19th – 20th September 2023

More details can be found on the following website:

https://www.cybersenate.com/control-systems-cybersecurity-usa/

SANS ICS Security Houston 2023

In recent years, we've seen highly sophisticated attacks on industrial systems that have interrupted operations and caused damage. As organizations implement new technology to improve their productivity and efficiency, adversaries evolve—and security teams are racing to find and adopt innovative approaches to safeguard systems and mitigate risk.

The industrial sector is a major target of cyber-attacks due to having little to no visibility into the assets they need to protect, and the lack of segmentation between IT and OT networks.

Listen to the leaders — learn to better defend your critical assets.

Virtual event; 25th – 30th September 2023

More details can be found on the following website:

https://www.sans.org/cyber-security-training-events/ics-security-houston-2023/

ICS incidents

Former employee charged for attacking water treatment plant

Former employee, Rambler Gallo, of the Discovery Bay Water Treatment Facility in California has been charged by a federal grand jury for intentionally attempting to cause a malfunction in the facility's safety and protection systems. Gallo, who had worked as an "instrumentation and control tech" for a private Massachusetts company contracted by Discovery Bay, allegedly installed remote control software on both his employer's systems and his personal computer. This enabled him to monitor readings and control the electromechanical processes of the water treatment facility. Despite resigning in January 2021, Gallo used his personal computer to remotely access the facility's network and deliberately attempted to cause harm by sending commands to uninstall critical software tools responsible for monitoring water pressure, filtration, and chemical levels.

The motivation behind Gallo's actions, which endangered the health and safety of 15,000 residents in the town, remains unclear. The U.S. Department of Justice has charged Gallo with one count of transmitting a program, information, code, and command to cause damage to a protected computer. If convicted, he faces a maximum statutory penalty of 10 years in prison and a fine of $250,000.

This case highlights the risks associated with improper access management to critical infrastructure systems, especially in public utilities that impact entire communities. Instances of poor cybersecurity practices can lead to significant damage when disgruntled employees with extensive access privileges or hackers exploit vulnerabilities. For instance, the 2021 attack on the water treatment system in Oldsmar, Florida, demonstrated the potential danger when threat actors attempted to increase the concentration of a dangerous chemical. This incident served as a wake-up call to the associated risks, and it was revealed that ransomware gangs regularly target public facilities nationwide to interrupt operations and profit from the disruptions.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/former-employee-charged-for-attacking-water-treatment-plant/

Israel's largest oil refinery website offline after DDoS attack

The website of BAZAN Group, Israel's largest oil refinery operator, has become inaccessible from most parts of the world due to a claimed cyber-attack by threat actors. The company, generating over $13.5 billion in annual revenue and employing more than 1,800 people, boasts a significant oil refining capacity. Incoming traffic to BAZAN Group's websites has been experiencing HTTP 502 errors or server refusals, effectively making the site unavailable to most visitors worldwide. However, it remains accessible from within Israel, indicating a possible geo-block implemented by BAZAN to counter the ongoing cyber-attack.

The hacktivist group known as 'Cyber Avengers' has taken responsibility for breaching BAZAN's network and leaked what appears to be screenshots of the company's SCADA systems. SCADA systems are crucial software applications used for monitoring and controlling industrial control systems. The leaked screenshots include diagrams of various industrial processes and PLC code. BAZAN has, in response, denied the authenticity of the leaked materials, labeling them as "entirely fabricated." The company states that it experienced a brief disruption on its image website due to a DDoS attack but asserts that no damage was observed on its servers or assets. BAZAN views the attack as an act of propaganda aimed at spreading misinformation and causing concern.

BAZAN emphasizes its commitment to cybersecurity and is closely cooperating with the Israeli National Cyber Directorate and other partners to monitor any suspicious activities. The company aims to ensure the safety and integrity of its operations in the face of potential cyber threats. The incident highlights the significant risks faced by critical infrastructure operators, like oil refineries, as they become targets of cyber-attacks. The protection of SCADA systems, which play a crucial role in industrial processes, is particularly vital to prevent potential disruptions and safeguard against unauthorized access to sensitive operational data.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/israels-largest-oil-refinery-website-offline-after-ddos-attack/

Book recommendation

IoT and OT Security Handbook

The Fourth Industrial Revolution, or Industry 4.0, is all about digital transformation, manufacturing, and production. The connected world we live in today, including industries, comes with several cybersecurity challenges that need immediate attention. This book takes you through the basics of IoT and OT architecture and helps you understand and mitigate these security challenges.

The book begins with an overview of the challenges faced in managing and securing IoT and OT devices in Industry 4.0. You'll then get to grips with the Purdue model of reference architecture, which will help you explore common cyber-attacks in IoT and OT environments. As you progress, you'll be introduced to Microsoft Defender for IoT and understand its capabilities in securing IoT and OT environments. Finally, you will discover best practices for achieving continuous monitoring and vulnerability management, as well as threat monitoring and hunting, and find out how to align your business model toward zero trust.

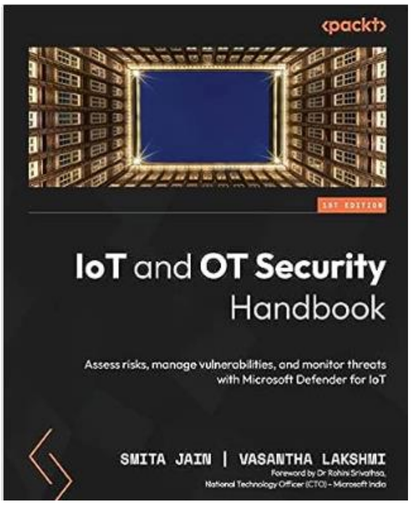
By the end of this security book, you'll be equipped with the knowledge and skills to efficiently secure IoT and OT environments using Microsoft Defender for IoT.

Authors/Editors: Smita Jain (Author), Vasantha Lakshmi (Author), Dr Rohini Srivathsa (Foreword)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.com/IoT-Security-Handbook-vulnerabilities-Microsoft/dp/1804619809


‹packt›
1ST EDITION
IoT and OT Security Handbook
Assess risks, manage vulnerabilities, and monitor threats with Microsoft Defender for IoT
SMITA JAIN | VASANTHA LAKSHMI
Foreword by Dr Rohini Srivathsa, National Technology Officer (CTO) - Microsoft India

ICS security news selection

House legislators introduce bipartisan bill to designate space as critical infrastructure

A group of bipartisan legislators has introduced legislation directing the Secretary of Homeland Security to designate space systems, services, and technology as a sector of critical infrastructure. The move would designate space as a dedicated sector of critical infrastructure, ensuring cogent security analyses of the space-based assets upon which society relies. The legislation is consistent with the Cyberspace Solarium Commission (CSC) 2.0’s recommendation that space systems be designated as a critical infrastructure sector.

Titled ‘Space Infrastructure Act,’ the legislation identifies that not later than 180 days after the date of the enactment of this section, the Secretary, in consultation with relevant agencies and departments of the federal government, the assistant to the president for Homeland Security and Counterterrorism, relevant federal advisory committees, and the executive director, shall issue guidance with respect to designating space systems, services, and technology as critical infrastructure. …

Source, and more information:

https://industrialcyber.co/regulation-standards-and-compliance/house-legislators-introduce-bipartisan-bill-to-designate-space-as-critical-infrastructure/

Ransomware Attacks on Industrial Organizations Doubled in Past Year: Report

The number of ransomware attacks targeting industrial organizations and infrastructure has doubled since the second quarter of 2022, according to data from industrial cybersecurity firm Dragos.

In a report analyzing data from the second quarter of 2023, Dragos said it saw 253 ransomware incidents, up 18% from the first quarter of 2023, when it observed 214 attacks.

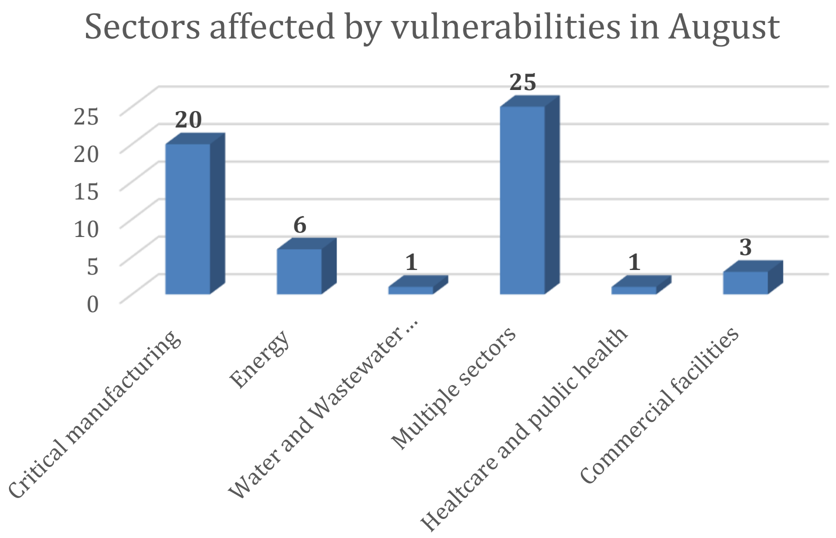
The company saw 189 ransomware incidents in the last quarter of 2022, a 30% increase from the 128 incidents in the third quarter of 2022. In the second quarter of 2022, the number dropped to 125 from 158 incidents in the first quarter. The drop was attributed at the time by Dragos to the shutdown of the Conti operation. …

Source, and more information:

https://www.securityweek.com/ransomware-attacks-on-industrial-organizations-doubled-in-past-year-report/

ICS vulnerabilities

In August 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:

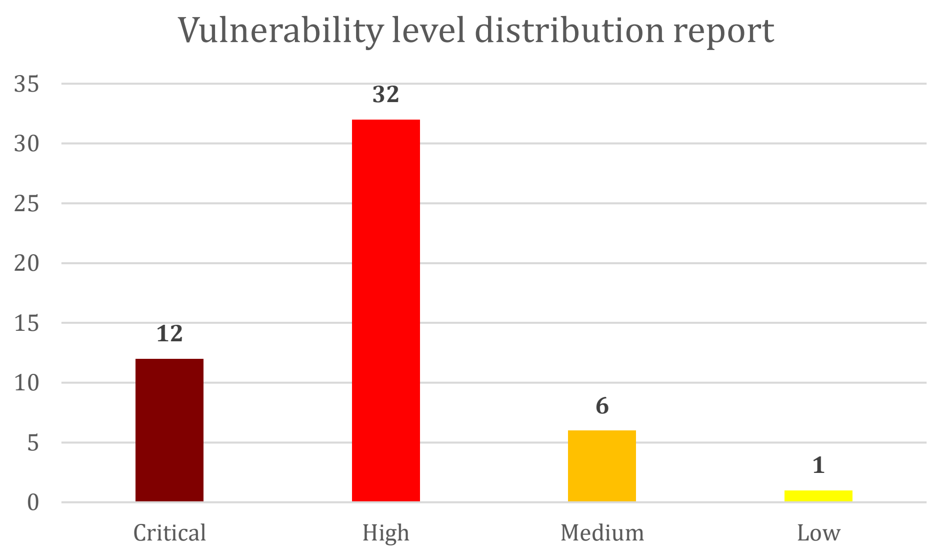


Average number of vulnerabilities per vulnerability report in August: **2,96**

Vulnerabilities/Exploitable remotely: **51/37**

The most common vulnerabilities in August:

Vulnerability	CWE number	Items
Out-of-bounds Read	CWE-125	9
Out-of-bounds Write	CWE-787	8
NULL Pointer Dereference	CWE-476	6
Improper Input Validation	CWE-20	6
Uncontrolled Resource Consumption	CWE-400	5



ICSA-23-243-01: **ARDEREG Sistemas SCADA**

Critical level vulnerability: SQL Injection.

ARDEREG Sistemas SCADA | CISA

ICSA-23-243-02: **GE Digital CIMPLICITY**

High level vulnerability: Process Control.

GE Digital CIMPLICITY | CISA

ICSA-23-243-03: **PTC Kepware KepServerEX**

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

PTC Kepware KepServerEX | CISA

ICSA-23-243-04: **Digi RealPort Protocol**

Critical level vulnerability: Use of Password Hash Instead of Password for Authentication.

Digi RealPort Protocol | CISA

ICSA-23-241-01: **PTC CodeBeamer**

High level vulnerability: Cross site scripting.

PTC Codebeamer | CISA

ICSA-23-236-01: **KNX Protocol**

High level vulnerability: Overly Restrictive Account Lockout Mechanism.

KNX Protocol | CISA

ICSA-23-236-02: **Opto 22 SNAP PAC S1**

High level vulnerabilities: Improper Restriction of Excessive Authentication Attempts, Weak Password Requirements, Improper Access Control, Uncontrolled Resource Consumption.

OPTO 22 SNAP PAC S1 | CISA

ICSA-23-236-03: **CODESYS Development System**

High level vulnerability: Uncontrolled Search Path Element.

CODESYS Development System | CISA

ICSA-23-236-04: **CODESYS Development System**

Low level vulnerability: Improper Restriction of Excessive Authentication Attempts.

CODESYS Development System | CISA

ICSA-23-236-05: **CODESYS Development System**

Critical level vulnerability: Insufficient Verification of Data Authenticity.

CODESYS Development System | CISA

ICSA-23-236-06: **Rockwell Automation Input/Output Modules**

High level vulnerability: Out-of-Bounds Write.

Rockwell Automation Select Distributed I/O Communication Modules | CISA

ICSA-23-234-01: **Hitachi Energy AFF66x**

Critical level vulnerabilities: Cross-site Scripting, Use of Insufficiently Random Values, Origin Validation Error, Integer Overflow or Wraparound, Uncontrolled Resource Consumption, NULL Pointer Dereference.

Hitachi Energy AFF66x | CISA

ICSA-23-234-02: **Trane Thermostats**

Medium level vulnerability: Injection.

Trane Thermostats | CISA

ICSA-23-234-03: **Rockwell Automation ThinManager ThinServer**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation ThinManager ThinServer | CISA

ICSA-23-138-02: **Mitsubishi Electric MELSEC WS Series (Update A)**

High level vulnerability: Active Debug Code.

Mitsubishi Electric MELSEC WS Series (UPDATE A) | CISA

ICSA-23-229-01: **ICONICS and Mitsubishi Electric Products**

Medium level vulnerabilities: Buffer Overflow, Out-of-Bounds Read, Observable Timing Discrepancy, Double Free, and NULL Pointer Dereference.

ICONICS and Mitsubishi Electric Products | CISA

ICSA-23-229-03: **Schnieder Electric PowerLogic ION7400 PM8000 ION9000 Power Meters**

High level vulnerability: Cleartext Transmission of Sensitive Information.

Schneider Electric PowerLogic ION7400 / PM8000 / ION8650 / ION8800 / ION9000 Power Meters | CISA

ICSA-23-229-04: **Walchem Intuition 9**

High level vulnerabilities: Missing Authentication for Critical Function, Improper Authentication.

Walchem Intuition 9 | CISA

ICSA-23-227-01: **Schneider Electric EcoStruxure Control Expert, Process Expert, Modicon**

High level vulnerability: Authentication Bypass by Capture-replay.

Schneider Electric EcoStruxure Control Expert, Process Expert, Modicon M340, M580 and M580 CPU | CISA

ICSA-23-227-02: **Rockwell Automation Armor PowerFlex**

High level vulnerability: Incorrect Calculation.

Rockwell Automation Armor PowerFlex | CISA

SSA-932528: **Siemens Solid Edge** **(Update: 1.1.)**

High level vulnerabilities: NULL Pointer Dereference, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use After Free.

SSA-932528 (siemens.com)

SSA-851884: **Siemens Mendix SAML Module** **(Update: 1.2.)**

Critical level vulnerability: Incorrect Implementation of Authentication Algorithm.

SSA-851884 (siemens.com)

SSA-794697: **SIMATIC S7-1500** **(Update: 1.2.)**

Critical level vulnerabilities: Multiple (37).

SSA-794697_V1.2 (siemens.com)

SSA-764801: **Siemens Tecnomatix Plant Simulation** **(Update: 1.1.)**

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-691715: **Siemens Products** **(Update: 1.2.)**

High level vulnerability: Improper Input Validation.

SSA-691715 (siemens.com)

SSA-686975: **Siemens Industrial Products using Intel CPUs** **(Update: 1.3.)**

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

SSA-686975 (siemens.com)

SSA-478960: **Siemens Web Server Login Page of Industrial Controllers** **(Update: 1.6.)**

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

SSA-478960 (siemens.com)

SSB-439005: **Siemens SIMATIC S7-1500 CPU** **(Update: 5.4.)**

Medium level vulnerabilities: Multiple.

SSB-439005_V5.4 (siemens.com)

SSA-306654: **Siemens Industrial Products (Update: 1.7.)**

High level vulnerabilities: Multiple (26 vulnerabilities).

SSA-306654_V1.7 (siemens.com)

SSA-223771: **Siemens SIPROTEC 5 Devices (Update: 1.3.)**

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

SSA-223771 (siemens.com)

SSA-180579: **APOGEE/TALON Field Panels before V3.5.5/V2.8.20 (Update: 1.1.)**

High level vulnerabilities: Out-of-bounds Write, Use of Out-of-range Pointer Offset, Improper Null Termination, Out-of-bounds Read, Access of Memory Location After End of Buffer, Predictable Exact Value from Previous Values, Use of Insufficiently Random Values, Improper Access Control.

SSA-180579 (siemens.com)

ICSA-23-222-01: **Siemens Solid Edge, JT2Go and Teamcenter Visualization**

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

Siemens Solid Edge, JT2Go, and Teamcenter Visualization | CISA

ICSA-23-222-02: **Siemens Parasolid Installer**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens Parasolid Installer | CISA

ICSA-23-222-03: **Siemens JT Open, JT Utilities, and Parasolid**

High level vulnerability: Out-of-bounds Read.

Siemens JT Open, JT Utilities, and Parasolid | CISA

ICSA-23-222-04: **Siemens Software Center**

High level vulnerabilities: Uncontrolled Search Path Element, Path Traversal.

Siemens Software Center | CISA

ICSA-23-222-05: **Siemens RUGGEDCOM CROSSBOW**

Critical level vulnerabilities: Out-of-bounds Read, Improper Privilege Management, SQL Injection, Missing Authentication for Critical Function.

Siemens RUGGEDCOM CROSSBOW | CISA

ICSA-23-222-06: **Siemens Parasolid and Teamcenter Visualization**

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

Siemens Parasolid and Teamcenter Visualization | CISA

ICSA-22-222-07: **Siemens Address Processing in SIMATIC**

High level vulnerability: Improper Input Validation.

Siemens Address Processing in SIMATIC | CISA

ICSA-23-222-08: **Resource Allocation in Siemens RUGGEDCOM**

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

Resource Allocation in Siemens RUGGEDCOM | CISA

ICSA-23-222-09: **Siemens OpenSSL RSA Decryption in SIMATIC**

Medium level vulnerability: Inadequate Encryption Strength.

Siemens OpenSSL RSA Decryption in SIMATIC | CISA

ICSA-23-222-10: **Siemens SICAM TOOLBOX II**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Execution with Unnecessary Privileges.

Siemens SICAM TOOLBOX II | CISA

ICSA-23-222-11: **Siemens Solid Edge SE2023**

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

Siemens Solid Edge SE2023 | CISA

ICSA-23-222-12: **Network Mirroring in Siemens RUGGEDCOM**

Critical level vulnerability: Incorrect Provision of Specified Functionality.

Network Mirroring in Siemens RUGGEDCOM | CISA

ICSA-23-220-01: **Schneider Electric IGSS**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric IGSS | CISA

ICSA-23-220-02: **Hitachi Energy RTU500 series**

High level vulnerability: Stack-based Buffer Overflow.

Hitachi Energy RTU500 series | CISA

ICSA-23-215-01: **Mitsubishi Electric GOT2000 and GOT SIMPLE**

Medium level vulnerability: Predictable Exact Value from Previous Values.

Mitsubishi Electric GOT2000 and GOT SIMPLE | CISA

ICSA-23-215-02: **Mitsubishi Electric GT and GOT Series Products**

High level vulnerability: Weak Encoding for Password.

Mitsubishi Electric GT and GOT Series Products | CISA

ICSA-23-215-03: **TEL-STER TelWin SCADA WebInterface**

High level vulnerability: Path Traversal.

TEL-STER TelWin SCADA WebInterface | CISA

ICSA-23-215-04: **Sensormatic Electronics VideoEdge**

High level vulnerability: Acceptance of Extraneous Untrusted Data with Trusted Data.

Sensormatic Electronics VideoEdge | CISA

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

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric CNC Series (Update A) | CISA

ICSA-23-213-01: **APSystems Altenergy Power Control**

Critical level vulnerability: OS Command Injection.

APSystems Altenergy Power Control | 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 August:

CISA Adds One Known Exploited Vulnerability to Catalog
CVE-2023-35081 Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability;
Link and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA and International Partner NCSC-NO Release Joint Cybersecurity Advisory on Threat Actors Exploiting Ivanti EPMM Vulnerabilities
Threat Actors Exploiting Ivanti EPMM Vulnerabilities, in response to the active exploitation of CVE-2023-35078 and CVE-2023-35081 affecting Ivanti Endpoint Manager Mobile (EPMM) (formerly known as MobileIron Core);
Link and more information:
CISA and International Partner NCSC-NO Release Joint Cybersecurity Advisory on Threat Actors Exploiting Ivanti EPMM Vulnerabilities | CISA

Mozilla Releases Security Updates for Multiple Products
Mozilla has released security updates to address vulnerabilities for Firefox 116, Firefox ESR 115.1, Firefox ESR 102.14, Thunderbird 115.1, and Thunderbird 102.14.
Link and more information:
Mozilla Releases Security Updates for Multiple Products | CISA

CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022
The U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and international partners are releasing a joint Cybersecurity Advisory (CSA), 2022 Top Routinely Exploited Vulnerabilities.
Link and more information:
CISA, NSA, FBI, and International Partners Release Joint CSA on Top Routinely Exploited Vulnerabilities of 2022 | CISA

CISA Releases its Cybersecurity Strategic Plan
CISA released a strategic plan to lay out how we will fulfill our cybersecurity mission over the next three years.
Link and more information:
CISA Releases its Cybersecurity Strategic Plan | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2017-18368 Zyxel P660HN-T1A Routers Command Injection Vulnerability

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Fortinet Releases Security Update for FortiOS

Fortinet has released a security update to address a vulnerability (CVE-2023-29182) affecting FortiOS.

Link and more information:

Fortinet Releases Security Update for FortiOS | CISA

Microsoft Releases August 2023 Security Updates

Microsoft has released updates to address multiple vulnerabilities in Microsoft software.

Link and more information:

Microsoft Releases August 2023 Security Updates | CISA

Adobe Releases Security Updates for Multiple Products

Adobe has released security updates to address multiple vulnerabilities in Adobe software.

Link and more information:

Adobe Releases Security Updates for Multiple Products | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-38180 Microsoft .NET Core and Visual Studio Denial of Service Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-24489 Citrix Content Collaboration ShareFile Improper Access Control Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan

CISA released the Remote Monitoring and Management (RMM) Cyber Defense Plan, the first proactive Plan developed by industry and government partners through the Joint Cyber Defense Collaborative (JCDC);

Link and more information:

CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan | CISA

Atlassian Releases Security Update for Confluence Server and Data Center

Atlassian has released its security bulletin for August 2023 to address a vulnerability in Confluence Server and Data Center, CVE-2023-28709;

Link and more information:

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

Cisco Releases Security Advisories for Multiple Products

Cisco has released security advisories for vulnerabilities affecting multiple Cisco products. A cyber threat actor can exploit some of these vulnerabilities to take control of an affected system or cause a denial-of service condition.

Link and more information:

Cisco Releases Security Advisories for Multiple Products | CISA

Juniper Releases Security Advisory for Multiple Vulnerabilities in Junos OS

Juniper has released a security advisory to address vulnerabilities in Junos OS on SRX Series and EX Series.

Link and more information:

Juniper Releases Security Advisory for Multiple Vulnerabilities in Junos OS | CISA

CISA Adds One Known Exploited Vulnerability to Catalog

CVE-2023-26359 Adobe ColdFusion Deserialization of Untrusted Data Vulnerability;

Link and more information:

CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA, NSA, and NIST Publish Factsheet on Quantum Readiness

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and National Institute of Standards and Technology (NIST) released a joint factsheet, Quantum-Readiness: Migration to Post-Quantum Cryptography.

Link and more information:
[CISA, NSA, and NIST Publish Factsheet on Quantum Readiness | CISA]

CISA Adds Two Known Exploited Vulnerabilities to Catalog
CVE-2023-38035: Ivanti Sentry Authentication Bypass Vulnerability
CVE-2023-27532: Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability;
Link and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Adds Two Known Exploited Vulnerabilities to Catalog
CVE-2023-38831 RARLAB WinRAR Code Execution Vulnerability
CVE-2023-32315 Ignite Realtime Openfire Path Traversal Vulnerability
Link and more information:
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA's VDP Platform 2022 Annual Report Showcases Success
Cybersecurity and Infrastructure Security Agency (CISA) released its inaugural Vulnerability Disclosure Policy (VDP) Platform 2022 Annual Report, highlighting the service's progress supporting vulnerability awareness and remediation across the Federal Civilian Executive Branch (FCEB).
Link and more information:
CISA's VDP Platform 2022 Annual Report Showcases Success | CISA

CISA Releases IOCs Associated with Malicious Barracuda Activity
CISA has released additional indicators of compromise (IOCs) associated with exploitation of CVE-2023-2868.
Link and more information:
CISA Releases IOCs Associated with Malicious Barracuda Activity | CISA

Mozilla Releases Security Updates for Firefox and Firefox ESR
Mozilla has released security updates to address vulnerabilities for Firefox 117, Firefox ESR 115.2, and Firefox ESR 102.15.
Link and more information:
Mozilla Releases Security Updates for Firefox and Firefox ESR | CISA

Juniper Networks Releases Security Advisory for Junos OS and Junos OS Evolved

Juniper Networks has released a security advisory to address a vulnerability for Junos OS and Junos OS Evolved. A cyber threat actor could exploit this vulnerability to cause a denial-of-service condition.

Link and more information:

Juniper Networks Releases Security Advisory for Junos OS and Junos OS Evolved | CISA

VMware Releases Security Updates for Aria Operations for Networks

CISA encourages users and administrators to review VMware Security Advisory VMSA-2023-0018 and apply the necessary updates.

Link and more information:

VMware Releases Security Updates for Aria Operations for Networks | CISA

CISA and FBI Publish Joint Advisory on QakBot Infrastructure

CISA and FBI released a joint Cybersecurity Advisory (CSA), Identification and Disruption of QakBot Infrastructure, to help organizations detect and protect against newly identified QakBot-related activity and malware. QakBot—also known as Qbot, Quackbot, Pinkslipbot, and TA570—is responsible for thousands of malware infections globally.

Link and more information:

CISA and FBI Publish Joint Advisory on QakBot Infrastructure | CISA

CISA and International Partners Release Malware Analysis Report on Infamous Chisel Mobile Malware

United Kingdom's National Cyber Security Centre (NCSC-UK), the United States' Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI), New Zealand's National Cyber Security Centre (NCSC-NZ), the Canadian Centre for Cyber Security (CCCS), and the Australian Signals Directorate (ASD) published a joint Malware Analysis Report (MAR), on Infamous Chisel, a new mobile malware targeting Android devices that has capabilities to enable unauthorized access to compromised devices, scan files, monitor traffic, and periodically steal sensitive information.

Link and more information:

CISA and International Partners Release Malware Analysis Report on Infamous Chisel Mobile Malware | CISA

CISA Warns of Hurricane-Related Scams

CISA urges users to remain on alert for malicious cyber activity following natural disasters, such as hurricanes, as attackers target disaster victims and concerned citizens by leveraging social engineering tactics, techniques, and procedures (TTPs).

Link and more information:

CISA Warns of Hurricane-Related Scams | CISA

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