2024 May, 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 podcasts

People listen more and more podcasts nowadays. Whether it's for our personal interests or for our professional development, the world of podcasts is a great possibility to be well informed. In this section, we bring together the ICS security podcasts from the previous month.

Dale Peterson

This podcast is named after and made by one of the most famous ICS security expert, Dale Peterson. It's made on Wednesdays on every week and the usual structure contains an opening monologue, interviews with guests and listener questions on topics that are on the leading, or even bleeding edge of OT and ICS security. The podcast is also interactive, so the listeners could ask question from Dale and the guests.

You can find all of Peterson's podcasts on the below URL.

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

This podcast is discussing major industrial cybersecurity topics and features industry experts covering everything from ransomware through critical infrastructure to supply chain attacks. Tune in to stay on top of the latest cybersecurity trends, threats and tactics. Hosted by Gary Cohen and Tyler Wall.

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

BEERISAC: OT/ICS Security Podcast Playlist

A curated playlist of Operational Technology and ICS Cyber Security related podcast episodes by ICS Security enthusiasts.

At this link, you can find numerous podcasts on the topic of ICS (Industrial Control Systems) created by various content producers. It's worth browsing through and listening to podcasts that are of interest to the organization or the readers of this newsletter themselves.

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/

ICS good practices, recommendations

SecurityWeek Cyber Insights 2024 Series

SecurityWeek's Cyber Insights is an annual series discussing the major pain points for cybersecurity practitioners. These pain points differ year by year in line with the evolving cyber ecosphere: this year the organizers include discussion on current pressures on the role of CISO, including the new SEC liability rules. Overall, Cyber Insights 2024 talks to hundreds of industry experts from dozens of companies covering seven primary topics. The purpose is to evaluate what is happening now, and to prepare for what is coming in 2024 and beyond.

Cyber Insights 2024 Topics

- OT, ICS and IIoT
- APIs – A Clear, Present, and Future Danger
- Artificial Intelligence (AI)
- Ransomware
- Supply Chain Security
- Quantum and the Cryptopocalypse
- The Role of the CISO

We recommend considering things relevant to the organization in the insights.

Source, links and more information available on the following link:

Cyber Insights 2024: OT, ICS and IIoT - SecurityWeek

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in June 2024:

- 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/

- 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/

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

- OT/IT Security Training

https://www.infosectrain.com/operational-technology-ot-training-courses/#courses

ICS conferences

In June 2024, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

NRECA's Co-op Cyber Tech

Industrial Defender will be attending the 2024 Co-op Cyber Tech Conference. Join us, June 11-13, 2024, for this 3-day technical conference with the goal of addressing cybersecurity in the cooperative space. This conference content specifically highlights co-op cyber and is designed to provide opportunities for peer-to-peer and industry-to-peer collaboration, skills development, and advancement.

Arlington, VA, USA; 11st – 13th June 2024

More details can be found on the following website:

https://www.industrialdefender.com/events/nrecas-co-op-cyber-tech

OT CYBERSECURITY SUMMIT

This event will focus on the leading international standards and conformance systems that are being used to keep operational technology (OT) safe and secure in industries such as energy, manufacturing, building automation, and more. New developments within the ISA/IEC 62443 standards series will be highlighted and technical training and certification programs designed to help you implement the standards into your business operations and workforce will be reviewed. Professionals involved in the security process should attend this event to learn more about workforce development strategies, hardware and software protection practices, and ways to improve infrastructure and data security measures.

London, UK; 17th – 21st June 2024

More details can be found on the following website:

https://dataconnectors.com/events/2024/ot-summit

ICS Security Summit & Training 2024

The Industrial Control System Cyber Security Summit & Training gathers experts and practitioners to discuss ICS security, offer SANS cybersecurity training, ICS NetWars, and networking opportunities. The annual summit shares ideas and techniques for protecting critical infrastructure, providing fresh perspectives. The expertise of speakers and quality attendees make the conference and after-hours discussions engaging and productive.

Orlando, FL, USA; 17th – 24th June 2024

More details can be found on the following website:

https://10times.com/ics-summit

ICS incidents

Ascension healthcare takes systems offline after cyberattack

Ascension, a prominent nonprofit healthcare system in the United States, has faced a significant setback as it grapples with a cybersecurity incident, prompting the organization to take several of its systems offline for investigation. With a vast network spanning 140 hospitals, 40 senior care facilities, and numerous affiliated providers across 19 states and the District of Columbia, Ascension plays a crucial role in healthcare delivery.

The discovery of unusual activity on select technology network systems on May 8 led Ascension to suspect a cybersecurity breach, prompting immediate response and initiation of investigative and remedial measures. Consequently, access to certain systems has been interrupted, affecting both internal operations and external connections with business partners. As a precautionary measure, Ascension advised its partners to suspend connections until further notice.

This disruption not only impacts operational efficiency but also extends to clinical services, exacerbating the challenges faced by healthcare providers and patients. Ascension has notified relevant authorities and engaged Mandiant incident response experts to navigate the incident and mitigate its impact.

The incident underscores the growing threat landscape facing the healthcare sector, as highlighted by recent warnings from the U.S. Department of Health and Human Services (HHS) regarding social engineering tactics employed by threat actors. These tactics target IT help desks to gain unauthorized access to corporate resources, posing significant risks to data security and patient care.

As Ascension continues to grapple with the aftermath of the cyber event, updates are forthcoming as the investigation progresses.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/ascension-healthcare-takes-systems-offline-after-cyberattack/

Book recommendation

Securing Operational Technology - The Purdue Model

In a world increasingly threatened by cyber-attacks, "Securing Operational Technology: A Comprehensive Guide to Implementing the Purdue Model" serves as a pivotal resource for any professional involved in protecting our critical infrastructures.

This book bridges the divide between information technology (IT) and operational technology (OT), introducing readers to the nuances that distinguish the two, and the imperative need for tailored cybersecurity solutions for OT systems.

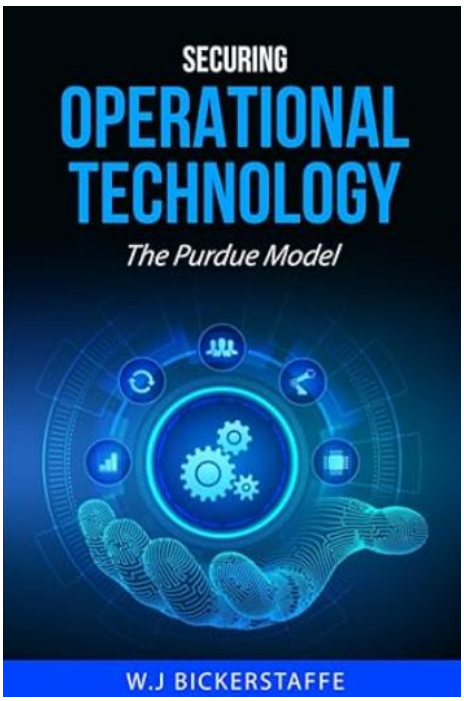
"Securing Operational Technology" presents an in-depth exploration of the Purdue Model, an essential framework that categorises OT systems into six distinctive levels. Each level, ranging from the sensory and actuating elements to enterprise resource planning systems, is meticulously dissected, with its unique security needs and control requirements detailed.

Author/Editor: William Bickerstaffe (Author)

Year of issue: 2023

The book is available at the following link:

https://www.amazon.ca/Securing-Operational-Technology-Cybersecurity-Approach/dp/B0CFWVZ2P9



ICS security news selection

US govt warns of pro-Russian hacktivists targeting water facilities

The US government is warning that pro-Russian hacktivists are seeking out and hacking into unsecured operational technology (OT) systems used to disrupt critical infrastructure operations.

The joint advisory comes from six US govt agencies, including CISA, FBI, NSA, EPA, DOE, USDA, and FDA, as well as the Multi-State Information Sharing and Analysis Center (MS-ISAC), Canada's Centre for Cyber Security (CCCS), and United Kingdom's National Cyber Security Centre (NCSC-UK).

OT devices are a combination of hardware and software platforms used to monitor and control physical processes or activities in manufacturing, critical infrastructure, and other industries. For example, water plants use OT devices to manage water treatment, distribution, and pressure to provide a continuous and safe water supply. …

Source and more information:

https://www.securityweek.com/cyber-insights-2024-ot-ics-and-iiot/

Honeywell: USB Malware Attacks on Industrial Orgs Becoming More Sophisticated

Industrial giant Honeywell has published its sixth annual report on the threat posed by USB-borne malware to industrial organizations, warning of an increase in sophistication.

The report is based on analysis conducted by the company's Global Analysis, Research and Defense (GARD) team using data collected by a security product designed to detect and block malware on USB drives used in customers' industrial environments.

Some data has remained largely unchanged in the past year compared to the two previous years. Of all the malware detected by Honeywell's product on USB drives, 31% was part of or associated with a campaign known to target industrial systems or companies. …

Source and more information:

https://www.securityweek.com/honeywell-usb-malware-attacks-on-industrial-orgs-becoming-more-sophisticated/

U.S. Government Releases New AI Security Guidelines for Critical Infrastructure

The U.S. government has unveiled new security guidelines aimed at bolstering critical infrastructure against artificial intelligence (AI)-related threats.

"These guidelines are informed by the whole-of-government effort to assess AI risks across all sixteen critical infrastructure sectors, and address threats both to and from, and involving AI systems," the Department of Homeland Security (DHS) said Monday.

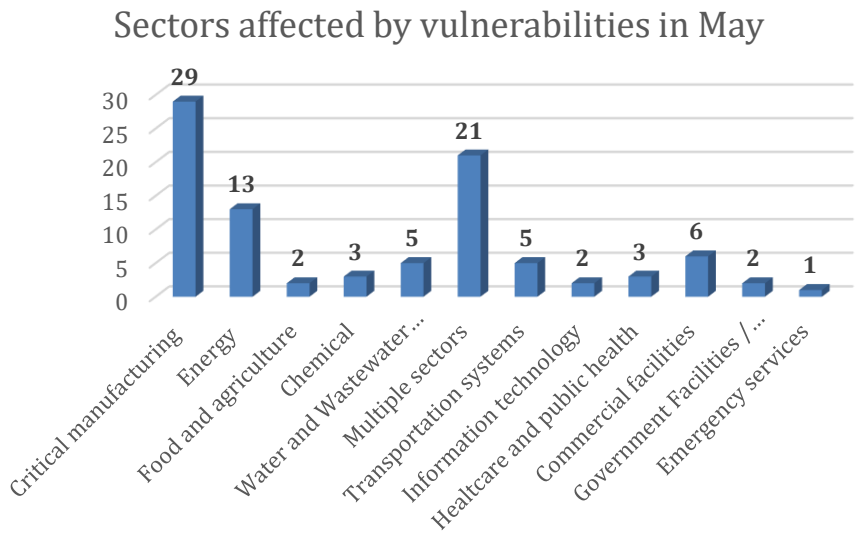
In addition, the agency said it's working to facilitate safe, responsible, and trustworthy use of the technology in a manner that does not infringe on individuals' privacy, civil rights, and civil liberties. ...

Source and more information:

https://thehackernews.com/2024/04/us-government-releases-new-ai-security.html

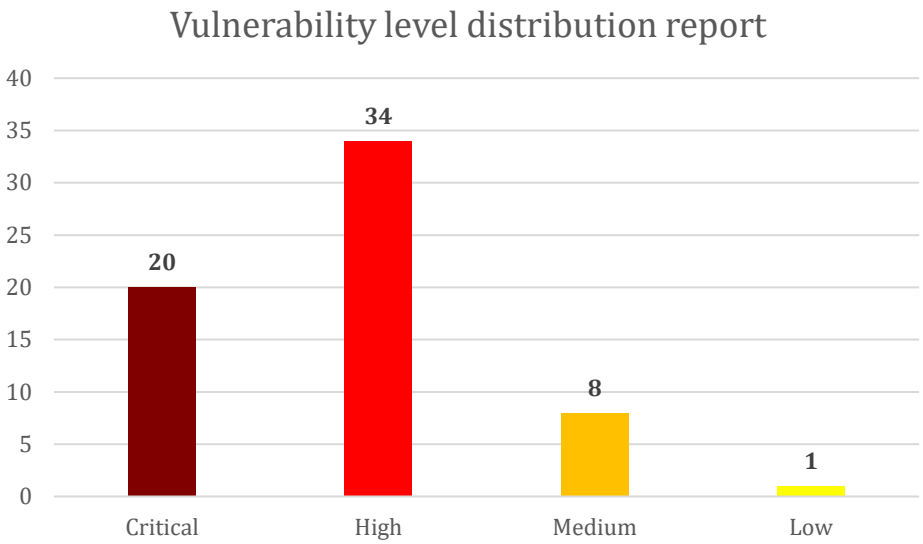
ICS vulnerabilities

In May 2024, 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 May:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	9
Uncontrolled Resource Consumption	CWE-400	8
Out-of-bounds Read	CWE-125	6
Stack-based Buffer Overflow	CWE-121	6
Use of Hard-coded Password	CWE-259	5
SQL Injection	CWE-89	5



ICSA-24-151-01: **LenelS2 NetBox**

Critical level vulnerabilities: Use of Hard-coded Password, OS Command Injection, Argument Injection.

LenelS2 NetBox | CISA

ICSA-24-151-02: **Fuji Electric Monitouch V-SFT**

High level vulnerabilities: Out-of-Bounds Write, Stack-Based Buffer Overflow.

Fuji Electric Monitouch V-SFT | CISA

ICSA-24-151-03: **Inosoft VisiWin**

High level vulnerability: Incorrect Default Permissions.

Inosoft VisiWin | CISA

ICSA-24-151-04: **Westermo EDW-100**

Critical level vulnerabilities: Use of Hard-coded Password, Insufficiently Protected Credentials.

Westermo EDW-100 | CISA

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

High level vulnerability: Improper Resource Shutdown or Release.

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

ICSMA-24-151-01: **Baxter Welch Allyn Configuration Tool**

Critical level vulnerability: Insufficiently Protected Credentials.

Baxter Welch Allyn Configuration Tool | CISA

ICSMA-24-151-02: **Baxter Welch Allyn Connex Spot Monitor**

Critical level vulnerability: Use of Default Cryptographic Key.

Baxter Welch Allyn Connex Spot Monitor | CISA

ICSA-24-149-01: **Campbell Scientific CSI Web Server**

Medium level vulnerabilities: Path Traversal, Weak Encoding for Password.

Campbell Scientific CSI Web Server | CISA

ICSA-24-144-01: **AutomationDirect Productivity PLCs**

Critical level vulnerabilities: Buffer Access with Incorrect Length Value, Out-of-bounds Write, Stack-based Buffer Overflow, Improper Access Control, Active Debug Code, Insufficient Verification of Data Authenticity.

AutomationDirect Productivity PLCs | CISA

ICSA-24-142-01: **LCDS LAquis SCADA**

High level vulnerability: Path Traversal.

LCDS LAquis SCADA | CISA

ICSA-24-137-01: **Siemens Parasolid**

High level vulnerabilities: Out-of-bounds Read, NULL Pointer Dereference.

Siemens Parasolid | CISA

ICSA-24-137-02: **Siemens SICAM Products**

High level vulnerabilities: Improper Null Termination, Command Injection, Cleartext Storage of Sensitive Information.

Siemens SICAM Products | CISA

ICSA-24-137-03: **Siemens Teamcenter Visualization and JT2Go**

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

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-24-137-04: **Siemens Polarion ALM**

High level vulnerability: Improper Access Control.

Siemens Polarion ALM | CISA

ICSA-24-137-05: **Siemens Simcenter Nastran**

High level vulnerability: Stack-based Buffer Overflow.

Siemens Simcenter Nastran | CISA

ICSA-24-137-06: **Siemens SIMATIC CN 4100 Before V3.0**

Critical level vulnerabilities: Use of Hard-coded Credentials, Use of Hard-coded Password, Missing Immutable Root of Trust in Hardware.

Siemens SIMATIC CN 4100 Before V3.0 | CISA

ICSA-24-137-07: **Siemens SIMATIC RTLS Locating Manager**

Critical level vulnerabilities: Improper Input Validation, Improper Check for Unusual or Exceptional Conditions, Uncontrolled Resource Consumption, Excessive Iteration, Allocation of Resources Without Limits or Throttling, Heap-based Buffer Overflow, External Control of File Name or Path, Missing Encryption of Sensitive Data, Download of Code Without Integrity Check, Use of Hard-coded Cryptographic Key, Incorrect Permission Assignment for Critical Resource, Cleartext Transmission of Sensitive Information, Insufficient Verification of Data Authenticity, Insufficiently Protected Credentials, Hidden Functionality.

Siemens SIMATIC RTLS Locating Manager | CISA

ICSA-24-137-08: **Siemens PS/IGES Parasolid Translator Component**

High level vulnerabilities: Out-of-bounds Read, Type Confusion, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens PS/IGES Parasolid Translator Component | CISA

ICSA-24-137-09: **Siemens Solid Edge**

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

Siemens Solid Edge | CISA

ICSA-24-137-10: **Siemens RUGGEDCOM CROSSBOW**

Critical level vulnerabilities: Missing Authorization, Improper Neutralization of Special Elements used in an SQL Command, Missing Authentication for Critical Function, External Control of File Name or Path, Improper Limitation of a Pathname to a Restricted Directory, Exposure of Sensitive Information to an Unauthorized Actor.

Siemens RUGGEDCOM CROSSBOW | CISA

ICSA-24-137-11: **Siemens RUGGEDCOM APE1808**

High level vulnerabilities: Insufficiently Protected Credentials, Improper Input Validation.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-137-12: **Siemens Desigo Fire Safety UL and Cerberus PRO UL Fire Protection Systems**

Critical level vulnerabilities: Classic Buffer Overflow, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Desigo Fire Safety UL and Cerberus PRO UL Fire Protection Systems | CISA

ICSA-24-137-13: **Siemens Industrial Products**

High level vulnerability: Out-of-bounds Read.

Siemens Industrial Products | CISA

ICSA-24-137-14: **Rockwell Automation FactoryTalk View SE**

High level vulnerability: Improper Input Validation.

Rockwell Automation FactoryTalk View SE | CISA

ICSA-23-044-01: **Mitsubishi Electric MELSEC iQ-R Series Safety CPU and SIL2 Process CPU (Update A)**

Medium level vulnerability: Incorrect Privilege Assignment.

Mitsubishi Electric MELSEC iQ-R Series Safety CPU and SIL2 Process CPU (Update A) | CISA

ICSA-24-074-14: **Mitsubishi Electric MELSEC-Q/L Series (Update A)**

Critical level vulnerabilities: Incorrect Pointer Scaling, Integer Overflow or Wraparound.

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

ICSMA-20-049-02: **GE Healthcare Ultrasound Products (Update A)**

High level vulnerabilities: Protection Mechanism Failure, Incorrect User Management.

GE Healthcare Ultrasound Products (Update A) | CISA

SSA-999588: **Siemens User Management Component (UMC) before V2.11.2 (Update 1.3.)**

High level vulnerabilities: Permissive Cross-domain Policy with Untrusted Domains, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Input Validation.

SSA-999588 (siemens.com)

SSA-968170: **Siemens SIMATIC STEP 7 V5.x and Derived Products (Update 1.3.)**

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

SSA-968170 (siemens.com)

SSA-935500: **Siemens FTP Server of Nucleus RTOS based APOGEE, TALON and Desigo PXC/PXM Products (Update 1.1.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-935500 (siemens.com)

SSA-871717: **Polarion ALM (Update 1.2.)**

High level vulnerabilities: Incorrect Default Permissions, Improper Authentication.

SSA-871717 (siemens.com)

SSA-832273: **Siemens RUGGEDCOM APE1808 devices (Update 1.2.)**

Critical level vulnerabilities: Heap-based Buffer Overflow, External Control of File Name or Path, Insufficiently Protected Credentials, Out-of-bounds Write, Stack-based Buffer Overflow, Improper Privilege Management, Uncontrolled Resource Consumption, Improper Authentication, Improper Certificate Validation, Use of Externally-Controlled Format String, Authorization Bypass Through User-Controlled Key, Exposure of Sensitive Information to an Unauthorized Actor.

SSA-832273 (siemens.com)

SSA-712929: **Siemens Industrial Products (Update 2.7.)**

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

SSA-712929 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update 1.8.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-691715: **Siemens Products (Update 1.5.)**

High level vulnerability: Improper Input Validation.

SSA-691715 (siemens.com)

SSA-665034: **Nozomi Guardian/CMC before 23.3.0 on Siemens RUGGEDCOM APE1808 devices (Update 1.1.)**

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

SSA-665034 (siemens.com)

SSA-647455: **Nozomi Guardian/CMC before 22.6.2 on Siemens RUGGEDCOM APE1808 devices (Update 1.2.)**

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)

SSA-593272: **Siemens Interniche IP-Stack based Industrial Devices (Update 2.1.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-593272 (siemens.com)

SSA-592380: **Siemens SIMATIC S7-1500 CPUs and related products (Update 1.2.)**

High level vulnerability: Use After Free.

SSA-592380 (siemens.com)

SSA-552874: **Siemens SIPROTEC 5 Devices (Update 1.4.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-552874 (siemens.com)

SSA-455250: **Siemens RUGGEDCOM APE1808 devices (Update 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-455250 (siemens.com)

SSA-446448: **Siemens PROFINET Stack Integrated on Interniche Stack (Update 2.0.)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

SSA-446448 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 1.1.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-382651: **Siemens Solid Edge (Update 1.1.)**

High level vulnerability: Out-of-bounds Read.

SSA-382651 (siemens.com)

SSA-322980: **Siemens SIPROTEC 5 Devices (Update 1.4.)**

High level vulnerability: NULL Pointer Dereference.

SSA-322980 (siemens.com)

SSA-292063: **Siemens RUGGEDCOM APE1808 devices (Update 1.1.)**

High level vulnerabilities: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Input Validation.

SSA-292063 (siemens.com)

SSA-265688: **Siemens SIMATIC S7-1500 TM MFP V1.1 (Update 1.1.)**

High level vulnerabilities: Improper Check for Unusual or Exceptional Conditions, Improper Input Validation, Use After Free, Out-of-bounds Write, Uncontrolled Resource Consumption.

SSA-265688 (siemens.com)

SSA-240541: **Siemens Industrial Products (Update 1.3.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-240541 (siemens.com)

SSA-225840: **Siemens Cerberus PRO EN Fire Protection Systems (Update 1.1.)**

Critical level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer.

SSA-225840 (siemens.com)

SSA-148641: **Siemens Mendix Runtime (Update 1.2.)**

Medium level vulnerability: Improper Access Control.

SSA-148641 (siemens.com)

ICSA-24-135-01: **Rockwell Automation FactoryTalk Remote Access**

High level vulnerability: Unquoted Search Path or Element.

Rockwell Automation FactoryTalk Remote Access | CISA

ICSA-24-135-02: **SUBNET PowerSYSTEM Center**

High level vulnerability: Reliance on Insufficiently Trustworthy Component.

SUBNET PowerSYSTEM Center | CISA

ICSA-24-135-03: **Johnson Controls Software House C-CURE 9000**

High level vulnerability: Insertion of Sensitive Information into Log File.

Johnson Controls Software House C-CURE 9000 | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products**

Medium level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write, Improper Privilege Management.

Mitsubishi Electric Multiple FA Engineering Software Products | CISA

ICSA-24-130-01: **Rockwell Automation FactoryTalk Historian SE**

High level vulnerabilities: Missing Release of Resource after Effective Lifetime, Improper Check or Handling of Exceptional Conditions.

Rockwell Automation FactoryTalk Historian SE | CISA

ICSA-24-130-02: **alpitronic Hypercharger EV Charger**

High level vulnerability: Use of Default Credentials.

alpitronic Hypercharger EV Charger | CISA

ICSA-24-130-03: **Delta Electronics InfraSuite Device Master**

Critical level vulnerability: Deserialization of Untrusted Data.

Delta Electronics InfraSuite Device Master | CISA

ICSA-24-107-03: **Rockwell Automation ControlLogix and GuardLogix (Update A)**

Critical level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix and GuardLogix (Update A) | CISA

ICSA-24-128-01: **PTC Codebeamer**

Medium level vulnerability: Cross-site Scripting.

PTC Codebeamer | CISA

ICSA-24-128-02: **SUBNET Substation Server**

High level vulnerability: Reliance on Insufficiently Trustworthy Component.

SUBNET Substation Server | CISA

ICSA-24-123-01: **CyberPower PowerPanel**

Critical level vulnerabilities: Use of Hard-coded Password, Relative Path Traversal, Use of Hard-coded Credentials, Active Debug Code, Storing Passwords in a Recoverable Format, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Use of Hard-coded Cryptographic Key, Improper Authorization.

CyberPower PowerPanel | CISA

ICSA-24-123-02: **Delta Electronics DIAEnergie**

Critical level vulnerabilities: SQL Injection, Path Traversal.

Delta Electronics DIAEnergie | CISA

ICSA-24-067-01: **Chirp Systems Chirp Access (Update C)**

Low level vulnerability: Use of Hard-coded Password.

Chirp Systems Chirp Access (Update C) | 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 2024 May:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-7028 GitLab Community and Enterprise Editions Improper Access Control Vulnerability;
CVE-2024-4671 Google Chromium in Visuals Use-After-Free Vulnerability;
CVE-2024-30051 Microsoft DWM Core Library Privilege Escalation Vulnerability;
CVE-2024-30040 Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability;
CVE-2014-100005 D-Link DIR-600 Router Cross-Site Request Forgery (CSRF) Vulnerability;
CVE-2021-40655 D-Link DIR-605 Router Information Disclosure Vulnerability;
CVE-2024-4761 Google Chromium V8 Out-of-Bounds Memory Write Vulnerability;
CVE-2024-4947 Google Chromium V8 Type Confusion Vulnerability;
CVE-2023-43208 NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability;
CVE-2020-17519 Apache Flink Improper Access Control Vulnerability;
CVE-2024-5274 Google Chromium V8 Type Confusion Vulnerability;
CVE-2024-4978 Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability;
CVE-2024-24919 Check Point Quantum Security Gateways Information Disclosure Vulnerability;
CVE-2024-1086 Linux Kernel Use-After-Free Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CERT/CC Reports R Programming Language Vulnerability
CERT Coordination Center (CERT/CC) has released information on a vulnerability in R programming language implementations (CVE-2024-27322). A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
CERT/CC Reports R Programming Language Vulnerability | CISA

CISA and Partners Release Fact Sheet on Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity

CISA, in collaboration with U.S. and international partners, published a joint fact sheet, Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity. This fact sheet provides information and mitigations associated with cyber operations conducted by pro-Russia hacktivists who seek to compromise industrial control systems (ICS) and small-scale operational technology (OT) systems in North American and European critical infrastructure sectors, including Water and Wastewater Systems, Dams, Energy, and Food and Agriculture Sectors.

Links and more information:

CISA and Partners Release Fact Sheet on Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity | CISA

CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate Directory Traversal Vulnerabilities

CISA and the Federal Bureau of Investigation (FBI) released a joint Secure by Design Alert, Eliminating Directory Traversal Vulnerabilities in Software. This Alert was crafted in response to recent well-publicized threat actor campaigns that exploited directory traversal vulnerabilities in software (e.g., CVE-2024-1708, CVE-2024-20345) to compromise users of the software—impacting critical infrastructure sectors, including the Healthcare and Public Health Sector.

Links and more information:

CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate Directory Traversal Vulnerabilities | CISA

ASD's ACSC, CISA, and Partners Release Secure by Design Guidance on Choosing Secure and Verifiable Technologies

Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), together with CISA, the Canadian Centre for Cyber Security (CCCS), the United Kingdom's National Cyber Security Centre (NCSC-UK), and the New Zealand National Cyber Security Centre (NCSC-NZ) are releasing the following guidance: Secure by Design Choosing Secure and Verifiable Technologies. This guidance was crafted to provide organizations with secure by design considerations when procuring digital products and services.

Links and more information:

ASD's ACSC, CISA, and Partners Release Secure by Design Guidance on Choosing Secure and Verifiable Technologies | CISA

CISA and Partners Release Advisory on Black Basta Ransomware

CISA, in partnership with the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released joint Cybersecurity Advisory (CSA) #StopRansomware: Black Basta to provide cybersecurity defenders tactics, techniques, and procedures (TTPs) and

indicators of compromise (IOCs) used by known Black Basta ransomware affiliates and identified through FBI investigations and third-party reporting.
Links and more information:
CISA and Partners Release Advisory on Black Basta Ransomware | CISA

CISA and Partners Release Guidance for Civil Society Organizations on Mitigating Cyber Threats with Limited Resources
CISA, in partnership with the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI) and international partners, released Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society. The joint guidance provides civil society organizations and individuals with recommended actions and mitigations to reduce the risk of cyber intrusions. Additionally, the guide encourages software manufactures to actively implement and publicly commit to Secure by Design practices that are necessary to help protect vulnerable and high-risk communities.
Links and more information:
CISA and Partners Release Guidance for Civil Society Organizations on Mitigating Cyber Threats with Limited Resources | CISA

Apple Releases Security Updates for Multiple Products
Apple has released security updates to address vulnerabilities in Safari, iOS, iPadOS, macOS, watchOS, and tvOS. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Apple Releases Security Updates for Multiple Products | CISA

Microsoft Releases May 2024 Security Updates
Microsoft 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.
Links and more information:
Microsoft Releases May 2024 Security Updates | CISA

Adobe Releases Security Updates for Multiple Products
Adobe has released security updates to address vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Adobe Releases Security Updates for Multiple Products | CISA

Cisco Releases Security Updates for Multiple Products
Cisco has released security updates to address vulnerabilities in Cisco software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

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

Rockwell Automation Encourages Customers to Assess and Secure Public-Internet-Exposed Assets
Rockwell Automation has released guidance encouraging users to remove connectivity on all Industrial Control Systems (ICS) devices connected to the public-facing internet to reduce exposure to unauthorized or malicious cyber activity.
Links and more information:
Rockwell Automation Encourages Customers to Assess and Secure Public-Internet-Exposed Assets | CISA

Cisco Releases May 2024 Cisco ASA, FMC, and FTD Software Security Publication
Cisco released a bundled publication for security advisories that address vulnerabilities in Cisco Adaptive Security Appliance (ASA), Firepower Management Center (FMC), and Firepower Threat Defense (FTD) software. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
Cisco Releases May 2024 Cisco ASA, FMC, and FTD Software Security Publication | CISA