2023 June, 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

IT and OT convergence is happening

When hackers inflicted a ransomware attack on Colonial Pipeline, shutting down fuel lines across the south-eastern United States and costing the company $4.4 million in ransom alone, the world took notice. From startups to corporate conglomerates, and from entry-level IT employees all the way up to the C-suite and boards, no one wanted to have another attack take place on their watch.

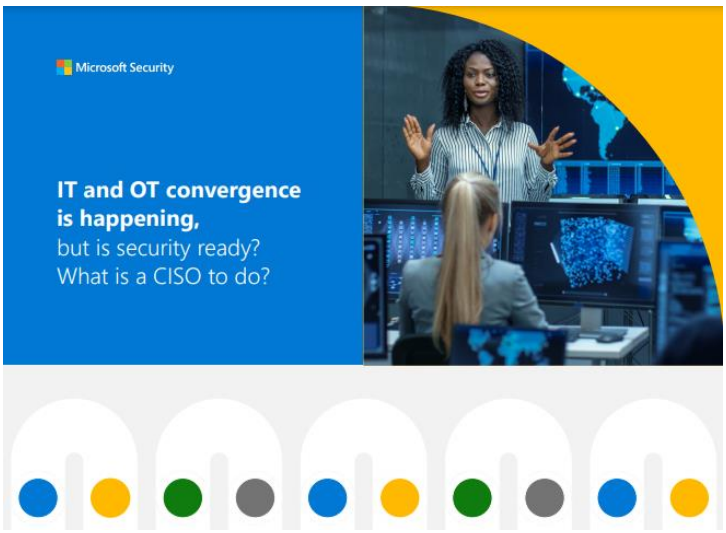
The costs to companies who are attacked go far beyond just the ransoms paid. Colonial Pipeline paid the ransom within hours of being attacked but was not fully operational until more than a week had passed. The shutdown caused widespread fuel shortages, panic buying, rescheduled flights, and increased gas prices. Whatever the industry, the risk to companies and their partners both upstream and downstream is real.

There is a massive growth trajectory for ransomware and extortion attacks in the coming years. The explosion of unmanaged devices and operational technology (OT) employed within organizations has dramatically increased the surface area for hackers to attack, and the often-mistaken belief among some C-suite executives is that the industrial systems have a similar level of protection as the rest of their IT network is only exacerbating matters. Of course, the CISO knows better!

Learn how to protect unmanaged IoT, ICS, and OT solutions in the Microsoft Defender for IoT e-book.

Source and more information available on the following link:

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5dSG5?culture=en-us&country=US



ICS trainings, education

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

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

49th NITSL Conference

The Nuclear Information Technology Strategic Leadership (NITSL) group is a nuclear industry group of all nuclear generation utilities that exchange information related to information technology management and quality issues

The annual NITSL conference brings together the leaders in the nuclear utility industry and regulatory agencies to address issues involved with information technology used in nuclear-powered utilities.

The four corner stones of NITSL are Software Quality Assurance, Cyber Security, Digital Controls and Infrastructure & Applications.

Scottsdale, AZ, USA; 10th – 13th July 2023

More details can be found on the following website:

https://industrialcyber.co/event/nitsl-conference/

Cyber Security for Critical Assets World Summit

CS4CA World will return virtually as a unique large-scale event to keep the critical asset community connected across the globe. As a worldwide 24-hour event, it will follow the sun by starting with speakers from the APAC region through to MEA, Europe, LatAm, finishing in North America.

Cyber attacks and cyber crime are increasing in number and sophistication across the world, leaving critical infrastructure organisations busy with reassessing their cyber risk while striving to maintain business continuity.

The summit offers dedicated sessions, allowing delegates to hone in on their specialist areas of interest, as well as topics addressing the issues that bind both IT & OT professionals, with a focus on advancing cybersecurity capacity building in the current geopolitical landscape.

Virtual Event; 11th July 2023

More details can be found on the following website:

https://world.cs4ca.com/?gclid=CjwKCAjw1YCkBhAOEiwA5aN4AYUeYZQyHDMaL4wIbqKknSFZom7-pKe5vxvqMzTrVE4SaMTPfqVS3BoC_VoQAvD_BwE

ICS incidents

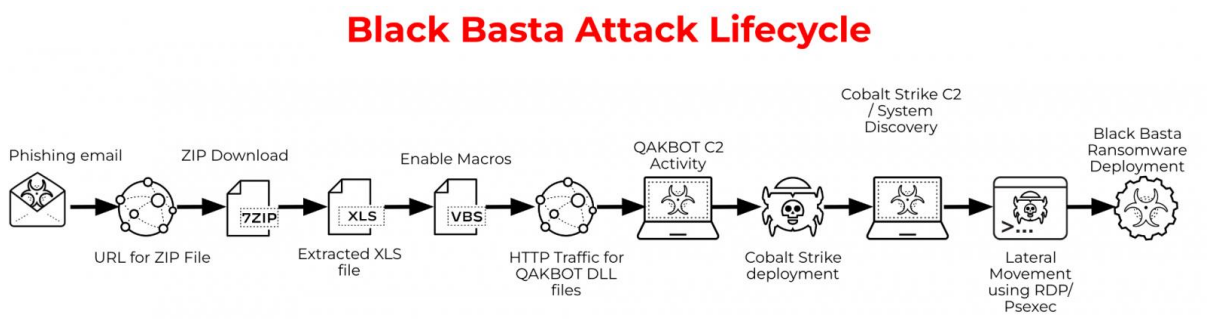
Multinational tech firm ABB hit by Black Basta ransomware attack

Swiss multinational company ABB, a leading electrification and automation technology provider, has suffered a Black Basta ransomware attack, reportedly impacting business operations.

Headquartered in Zurich, Switzerland, ABB employs approximately 105,000 employees and has $29.4 billion in revenue for 2022. As part of its services, the company develops industrial control systems (ICS) and SCADA systems for manufacturing and energy suppliers.

On May 7th, the company fell victim to a cyber attack conducted by the Black Basta ransomware gang, a cybercrime group that surfaced in April 2022. The ransomware attack has affected the company's Windows Active Directory, affecting hundreds of devices. In response to the attack, ABB terminated VPN connections with its customers to prevent the spread of the ransomware to other networks.

The attack reportedly disrupts the company's operations, delaying projects and impacting the factories. To address the situation, ABB has taken, and continues to take, measures to contain the incident. Such containment measures have resulted in some disruptions to its operations which the company is addressing. The vast majority of its systems and factories are now up and running and ABB continues to serve its customers in a secure manner.



The source is available on the following link:

https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/

Book recommendation

Industrial Security

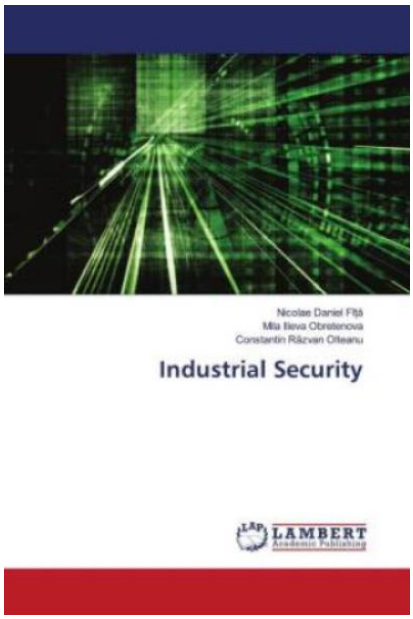
The present book entitled INDUSTRIAL SECURITY debates current issues of security of industrial objectives in the Romanian economy, in the context of ensuring economic and national security. The book brings an element of novelty through the Integrated System of Industrial Security, which must be implemented by any European company of strategic importance and which is composed of: Risk Management; Security and Protection of Critical Infrastructures Management; Occupational Health and Safety Management; Anti-Bribery Management; Business Continuity Management; Resilience. The authors hope that this book will be useful to all specialists and national and European decision-makers who are responsible for ensuring and increasing industrial and implicit economic security.

Authors/Editors: Mila Ilieva Obretenova, Nicolae Daniel FÎȚĂ, Constantin Răzvan Olteanu

Year of issue: 2023

The book is available at the following link:

https://www.walmart.com/ip/Industrial-Security-Paperback/1111295508?wmlspartner=wlpa&selectedSellerId=0



ICS security news selection

Forescout predicts that AI-assisted attacks will soon target OT, unmanaged devices

Forescout Technologies outlined how AI-assisted attacks are coming to target OT (operational technology) and unmanaged devices. The shift comes as hackers are exploiting publicly available proof-of-concept (PoCs), increasing the versatility and potentially the damage of existing malicious code, though it still takes some time and effort from threat actors. These developments demonstrate how generative AI can be used to improve productivity, while also being deployed for nefarious purposes.

"Malicious code is not difficult to find these days, even for OT, IoT, and other embedded and unmanaged devices," Amine Amri and Daniel dos Santos, researchers at Forescout Vedere Labs, wrote in a Wednesday blog post. "Public exploit proofs-of-concept (PoCs) for IP camera vulnerabilities are routinely used by Chinese APTs, popular building automation devices are targeted by hacktivists and unpatched routers used for Russian espionage." …

Source, and more information:

https://industrialcyber.co/ai/forescout-predicts-that-ai-assisted-attacks-will-soon-target-ot-unmanaged-devices/

New Russia-Linked CosmicEnergy ICS Malware Could Disrupt Electric Grids

Mandiant on May detailed a new piece of malware that appears to be linked to Russia and is designed to target industrial control systems (ICS), specifically in an effort to cause electric grid disruption.

Named CosmicEnergy, the latest malware family targeting operational technology (OT) is designed to interact with IEC 60870-5-104 (IEC-104) devices, sending remote commands to tamper with the actuation of power line switches and circuit breakers in an effort to cause power disruption. Mandiant believes it "poses a plausible threat to affected electric grid assets". …

Source, and more information:

https://www.securityweek.com/new-russia-linked-cosmicenergy-ics-malware-can-disrupt-electric-grid/

Why Critical Infrastructure Remains a Ransomware Target

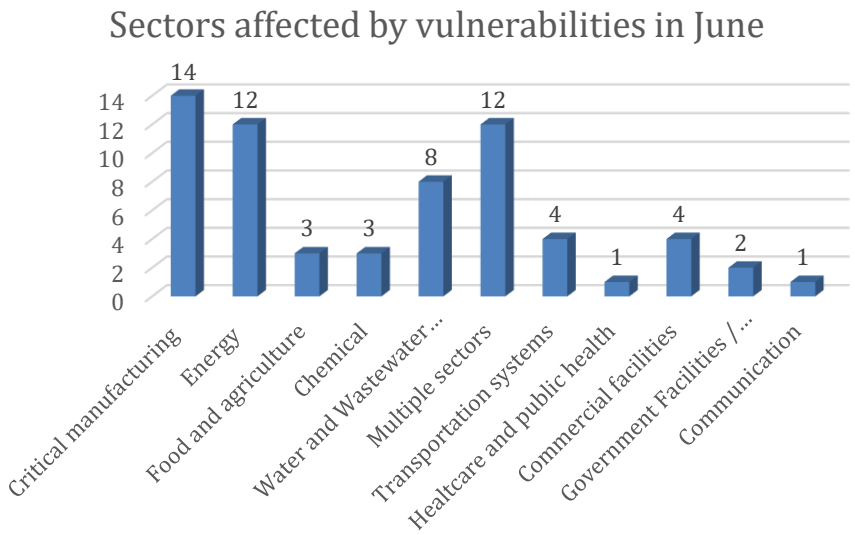
There continues to be a lot of pressure on security leaders to do more with less, but today's sophisticated and frequent cyberattacks only exacerbate the situation. And the bad news is these cyber incidents, particularly ransomware attacks, are not going away any time soon. In fact, they are becoming more prevalent in areas like critical infrastructure, supply chain, and financial institutions. For example, the Cybersecurity and Infrastructure Security Agency (CISA) observed ransomware incidents against 14 of the 16 US critical infrastructure sectors in 2021. …

Source, and more information:

https://www.darkreading.com/vulnerabilities-threats/why-critical-infrastructure-remains-a-ransomware-target

ICS vulnerabilities

In June 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:

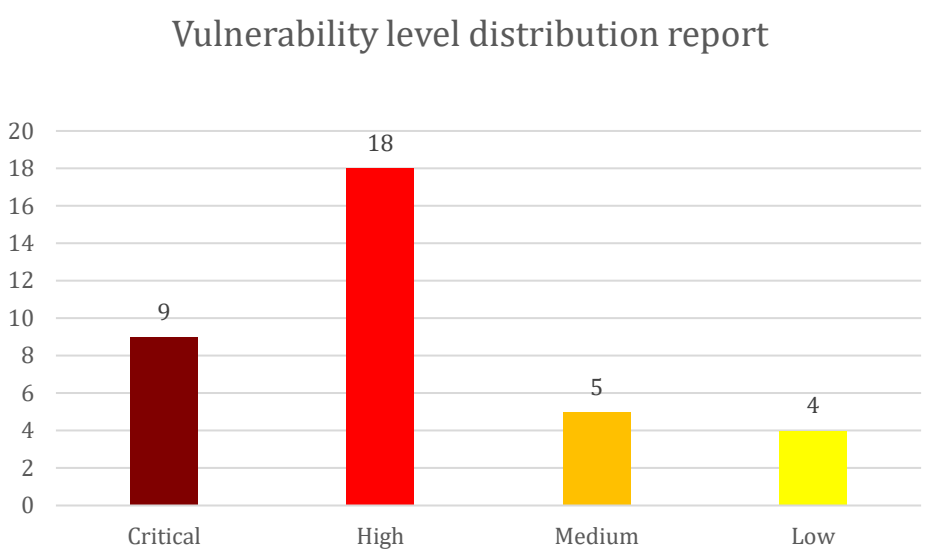


Average number of vulnerabilities per vulnerability report in June: **3,44**

Vulnerabilities/Exploitable remotely: **36/23**

The most common vulnerabilities in June:

Vulnerability	CWE number	Items
Out-of-bounds Read	CWE-125	6
Improper Input Validation	CWE-20	5
Use of Hard-coded Credentials	CWE-798	4



ICSA-23-180-04: **Mitsubishi Electric MELSEC-F Series**

High level vulnerability: Authentication Bypass by Capture-replay.

Mitsubishi Electric MELSEC-F Series | CISA

ICSA-23-180-03: **Ovarro TBox RTUs**

High level vulnerabilities: Missing Authorization, Use of Broken or Risky Cryptographic Algorithm, Inclusion of Functionality from Untrusted Control Sphere, Insufficient Entropy, Improper Authorization, Plaintext Storage of a Password.

Ovarro TBox RTUs | CISA

ICSA-23-180-02: **Schneider Electric EcoStruxure Operator Terminal Expert**

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

Schneider Electric EcoStruxure Operator Terminal Expert | CISA

ICSA-23-180-01: **Delta Electronics InfraSuite Device Master**

High level vulnerabilities: Improper Access Control, Deserialization of Untrusted Data.

Delta Electronics InfraSuite Device Master | CISA

ICSA-23-178-01: **Hitachi Energy FOXMAN-UN and UNEM Products**

Low level vulnerability: Improper Output Neutralization for Logs.

Hitachi Energy FOXMAN-UN and UNEM Products | CISA

ICSA-23-173-03: **SpiderControl SCADAWebServer**

Low level vulnerability: Path Traversal.

SpiderControl SCADAWebServer | CISA

ICSA-23-173-02: **Advantech R-SeeNet**

Critical level vulnerabilities: Hard Coded Password, External Control of File Name or Path.

Advantech R-SeeNet | CISA

ICSA-23-171-02: **Enphase Installer Toolkit Android App**

High level vulnerability: Use of Hard-coded Credentials.

Enphase Installer Toolkit Android App | CISA

ICSA-23-171-01: **Enphase Envoy**

Medium level vulnerability: OS Command Injection.

Enphase Envoy | CISA

ICSA-23-166-14: **Siemens Teamcenter Visualization and JT2Go**

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

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-23-166-13: **Siemens SICAM A8000 Devices**

High level vulnerabilities: Command Injection, Use of Hard-coded Credentials, Exposed Dangerous Method or Function.

Siemens SICAM A8000 Devices | CISA

ICSA-23-166-12: **Siemens SINAMICS Medium Voltage Products**

Critical level vulnerabilities: Out-of-bounds Write, Out-of-bounds Read, Use After Free, Improper Authentication, OS Command Injection, Improper Certificate Validation, Improper Resource Shutdown or Release, Allocation of Resources Without Limits or Throttling, Incorrect Default Permissions, Improper Validation of Syntactic Correctness of Input, Improper Input Validation.

Siemens SINAMICS Medium Voltage Products | CISA

ICSA-23-166-11: **Siemens SIMATIC S7-1500 TM MFP Linux Kernel**

Critical level vulnerabilities: Multiple vulnerabilities (33 different kind of vulnerabilities).

Siemens SIMATIC S7-1500 TM MFP Linux Kernel | CISA

ICSA-23-166-10: **Siemens SIMATIC S7-1500 TM MFP BIOS**

Critical level vulnerabilities: Improper Input Validation, Out-of-bounds Read, Use After Free, Out-of-bounds Write, Infinite Loop, Reachable Assertion, Off-by-one Error, Incorrect Default Permissions, Double Free, Improper Handling of Exceptional Conditions, Integer Overflow or Wraparound, NULL Pointer Dereference, Release of Invalid Pointer or Reference, Race Condition, Improper Restriction of Operations within the Bounds of a Memory Buffer, Non-exit on Failed Initialization, Missing Encryption of Sensitive Data, Classic Buffer Overflow, Uncontrolled Resource Consumption.

Siemens SIMATIC S7-1500 TM MFP BIOS | CISA

ICSA-23-166-09: **Siemens Solid Edge**

High level vulnerability: Out-of-bounds Read.

Siemens Solid Edge | CISA

ICSA-23-166-08: **Siemens SIMATIC STEP 7 and Derived Products**

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

Siemens SIMATIC STEP 7 and Derived Products | CISA

ICSA-23-166-07: **Siemens SIMATIC WinCC V7**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SIMATIC WinCC V7 | CISA

ICSA-23-166-06: **Siemens TIA Portal**

Medium level vulnerability: Protection Mechanism Failure.

Siemens TIA Portal | CISA

ICSA-23-166-05: **Siemens SIMATIC WinCC**

Low level vulnerability: Use of Obsolete Function.

Siemens SIMATIC WinCC | CISA

ICSA-23-166-04: **Siemens SIMOTION**

Low level vulnerability: Exposure of Sensitive Information Due to Incompatible Policies.

Siemens SIMOTION | CISA

ICSA-23-166-03: **Siemens SICAM Q200 Devices**

Critical level vulnerabilities: Session Fixation, Improper Input Validation, Cross-Site Request Forgery, Incorrect Permission Assignment for Critical Resource.

Siemens SICAM Q200 Devices | CISA

ICSA-23-166-02: **Advantech WebAccess/SCADA**

Critical level vulnerability: Untrusted Pointer Dereference.

Advantech WebAccess/SCADA | CISA

ICSA-23-166-01: **SUBNET PowerSYSTEM Center**

Medium level vulnerabilities: Cross-site Scripting, Authentication Bypass by Capture-replay.

SUBNET PowerSYSTEM Center | CISA

ICSA-23-164-04: **Rockwell Automation FactoryTalk Transaction Manager**

High level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation FactoryTalk Transaction Manager | CISA

ICSA-23-164-03: **Rockwell Automation FactoryTalk Edge Gateway**

High level vulnerability: Out-of-bounds Read.

Rockwell Automation FactoryTalk Edge Gateway | CISA

ICSA-23-164-02: **Rockwell Automation FactoryTalk Services Platform**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Improper Authentication, Origin Validation Error.

Rockwell Automation FactoryTalk Services Platform | CISA

ICSA-23-164-01: **Datalogics Library Third-Party**

Medium level vulnerability: Stack-based buffer overflow.

Datalogics Library Third-Party | CISA

ICSA-23-159-02: **Sensormatic Electronics Illustra Pro Gen 4**

High level vulnerability: Active Debug Code.

Sensormatic Electronics Illustra Pro Gen 4 | CISA

ICSA-23-159-01: **Atlas Copco Power Focus 6000**

Medium level vulnerabilities: Cleartext Storage of Sensitive Information, Small Space of Random Values, Cleartext Transmission of Sensitive Information.

Atlas Copco Power Focus 6000 | CISA

ICSA-23-157-02: **Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series**

High level vulnerabilities: Weak Password Requirements, Use of Hard-coded Password, Missing Password Field Masking, Unrestricted Upload of File with Dangerous Type.

Mitsubishi Electric MELSEC iQ-R Series/iQ-F Series | CISA

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

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

Delta Electronics CNCSoft-B DOPSoft | CISA

ICSA-22-256-03: **Delta Electronics DIAEnergie (Update A)**

Critical level vulnerability: Use of Hard-coded Credentials.

Delta Electronics DIAEnergie (Update A) | CISA

ICSA-22-333-05: **Mitsubishi Electric FA Engineering Software (Update A)**

Critical level vulnerabilities: Cleartext Storage of Sensitive Information, Use of Hard-coded Password, Insufficiently Protected Credentials, Use of Hard-coded Cryptographic Key, Cleartext Storage of Sensitive Information in Memory.

Mitsubishi Electric FA Engineering Software (Update A) | CISA

ICSA-21-096-01: **Hitachi Energy Relion 670 650 SAM600IO (Update B)**

High level vulnerability: Improper Input Validation.

Hitachi Energy Relion 670, 650 and SAM600-IO (Update B) | CISA

ICSA-23-152-02: **HID Global SAFE**

High level vulnerability: Modification of Assumed-Immutable Data.

https://www.cisa.gov/news-events/ics-advisories/icsa-23-152-02

ICSA-23-152-01: **Advantech WebAccess/SCADA**

High level vulnerabilities: Improper Control of Generation of Code ('Code Injection'), Unrestricted Upload of File with Dangerous Type.

https://www.cisa.gov/news-events/ics-advisories/icsa-23-152-01

The vulnerability reports contain more detailed information, which can be found on the following website:

Cybersecurity Alerts & Advisories | CISA

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 June:

CL0P Ransomware Gang Exploits MOVEit Vulnerability

ransomware; MOVEit Transfer Advisory; exploit; StopRansomware; CL0P Ransomware Gang; indicators of compromise

Link and more information:

CISA and FBI Release #StopRansomware: CL0P Ransomware Gang Exploits MOVEit Vulnerability | CISA

Mitigating the Risk from Internet-Exposed Management Interfaces

Binding Operational Directive; Interface security; Zero Trust

Link and more information:

CISA Issues BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces | CISA