2022 December, 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 2
ICS trainings, education 3
ICS conferences 5
ICS incidents 6
Book recommendation 7
ICS security news selection 8
ICS vulnerabilities 10
ICS alerts 20

ICS good practices, recommendations

NIS Investments 2022

This report marks the third iteration of ENISA's NIS Investments report, which collects data on how Operators of Essential Services (OES) and Digital Service Providers (DSP) identified in the European Union's directive on security of network and information systems (NIS Directive) invest their cybersecurity budgets and how this investment has been influenced by the NIS Directive. In addition, global cybersecurity market trends are presented through Gartner security data and insights observed globally and in the EU, in order to provide a better understanding of the relevant dynamics.

This year's report presents data collected from 1080 OES/DSPs from all 27 EU Member States and can now provide a historical dataset that allows for year-on-year comparison and identification of trends. Moreover, sectorial deep dives were conducted for the Energy and Health sectors. Overall, a number of absolute values, such as IT and Information Security (IS) budgets or % of IT budgets spent on IS seem to be significantly lower compared to last year. This can be attributed to the composition of the survey sample and to the higher representation of OES from the Energy and Health sectors due to the sectorial deep dives, but also to the macroeconomic environment, such as the COVID-19 impact on the respective budgets.

We recommend analysing the report, if your organization is one from the mentioned sectors.

Source and more information available on the following link:

https://www.enisa.europa.eu/publications/nis-investments-2022

ICS trainings, education

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

ICS conferences

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

CS4CA MENA 2023

As OT environments continue to converge with IT networks the need to secure these technologies to support continuous uptime and safety, has never been more critical. In particular, for business leaders in the Oil & Gas, Chemical, Healthcare, Mining, Utility, Maritime, and other critical industries. With this in mind, CS4CA MENA summit will explore all aspects of IT & OT security with a focus on digitally transforming critical infrastructure. The summit will bring together some of the brightest minds in the industry, uniting 100+ IT & OT security leaders in Dubai for 2 days of insight building, strategy planning and expert knowledge exchange on 24th – 25th January 2023.

Dubai United Arab Emirates; 24th – 25th January 2023

More details can be found on the following website:

https://cyware.com/cyber-security-events/conference/cs4ca-mena-2023-ad5dd437/

IT Contracts 2023

This time, you'll be able to hear about the trends we're seeing as a result of standardized IT services and the cloud transition. You will also be able to hear about the new questions that we anticipate will be addressed as IT security issues become even more important as a result of general development, the global situation, and the new NIS2 Directive.

Copenhagen, Denmark; 24th January 2023

More details can be found on the following website:

https://www.eventyco.com/event/it-contracts-2023-copenhagen-denmark

ICS incidents

Trains stopped in Denmark due to a cyber attack

The end of October there was an incident in Denmark, trains stopped for hours due to a cyberattack.

The hackers targeted not directly DSB (Danish state railways). The attack targeted a third party, which is an IT service provider (Supeo) and serviced the Digital Backpack 2 platform, what allows train drivers to access operationally critical information using an iPhone or iPad.

Supeo suffered a massive ransomware attack, and the company decided to shut down the servers. That was the reason behind the non-functioning of the platform what train drivers use to access critical operational information, such as speed limits and information on work being done to the railroad.

The company said that maybe hacking OT (Operational Technology) systems was the aim of the attackers.

DSB's CSO mentioned that it was not clear who was behind the attack, but that investigations were ongoing.

This incident shows that third-party risk management is very important.

The source and more information are available on the following links:

https://www.securityweek.com/cyberattack-causes-trains-stop-denmark

https://cybernews.com/news/cyberattack-paralyzed-danish-railways/

https://securityaffairs.co/wordpress/138127/cyber-crime/cyberattack-blocked-trains-denmark.html

Forrás: https://cybernews.com/news/cyberattack-paralyzed-danish-railways/

Book recommendation

Critical Infrastructure Security and Resilience

The World Economic Forum regards the threat of cyber-attacks as one of the top five global risks confronting nations of the world today. Cyber-attacks are increasingly targeting the core functions of the nations' economies in the world. The threat to attack critical infrastructure, disrupt critical services, and induce a wide range of damage is becoming more difficult to defend against.

The book "Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare" examines the current cyber threat landscape and discusses the strategies being used by governments and corporations to protect against these threats. The book first provides a historical reference, detailing the emergence of viruses, worms, malware, and other cyber threats that created the need for the cybersecurity field. It then discusses the vulnerabilities of our critical infrastructures, the broad arsenal of cyber-attack tools, and the various engineering design issues involved in protecting our infrastructures. It goes on to cover cyber intelligence tactics, recent examples of cyber conflict and warfare, and the key issues in formulating a national strategy to defend against cyber warfare.

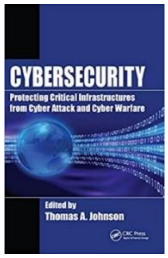
The book also discusses how to assess and measure the cost of cybersecurity. It examines the many associated cost factors and presents the results of several important industry-based economic studies of security breaches that have occurred within many nations. The book concludes with a look at future trends in cybersecurity. It discusses the potential impact of industry-wide transformational changes, such as virtualization, social media, cloud computing, structured and unstructured data, big data, and data analytics.

Authors/Editors: Thomas A. Johnson

Year of issue: 2015

The book is available at the following link:

https://www.amazon.com/Cybersecurity-Protecting-Critical-Infrastructures-Warfare/dp/1482239221



ICS security news selection

How IoT is changing the threat landscape for businesses

Where IoT-enabled devices connect to wider networks, their potential functionalities are immense, with countless applications across various industries, including production and manufacturing, healthcare, finance, and energy.

In the Help Net Security video, Paul Keely, Chief Cloud Officer at Open Systems, talks about how organizations that employ IoT technology have improved their business efficiency.

Still, all this data introduces a new challenge – security. While IoT presents organizations with new ways to advance and optimize, the continuous exchange of data and network connectivity creates opportunities for that information to be compromised. …

Source, the video and more information:

https://www.helpnetsecurity.com/2022/12/08/iot-threat-landscape-businesses-video/

Chinese Hackers Target Middle East Telecoms in Latest Cyber Attacks

A malicious campaign targeting the Middle East is likely linked to BackdoorDiplomacy, an advanced persistent threat (APT) group with ties to China.

The espionage activity, directed against a telecom company in the region, is said to have commenced on August 19, 2021 through the successful exploitation of ProxyShell flaws in the Microsoft Exchange Server.

Initial compromise leveraged binaries vulnerable to side-loading techniques, followed by using a mix of legitimate and bespoke tools to conduct reconnaissance, harvest data, move laterally across the environment, and evade detection. …

Source and more information:

https://thehackernews.com/2022/12/chinese-hackers-target-middle-east.html

CISA Updates Infrastructure Resilience Planning Framework

The US Cybersecurity and Infrastructure Security Agency (CISA) this week announced the addition of new tools and guidance to the Infrastructure Resilience Planning Framework (IRPF).

Initially released in 2021, the IRPF (PDF) is meant for state, local, tribal, and territorial (SLTT) entities looking to include critical infrastructure security and resilience in their planning, in the face of evolving threats. IRPF can be used by any organization to improve resilience planning.

The framework can help understand and communicate on how the community benefits from infrastructure resilience; identify the impact of threats and hazards; prepare relevant entities for evolving threats and hazards; integrate critical infrastructure security and resilience into planning and investment decisions; and recover faster from disruptions. …

Source and more information:

https://www.securityweek.com/cisa-updates-infrastructure-resilience-planning-framework

Microsoft Warns of Boa Web Server Risks After Hackers Target It in Power Grid Attacks

Microsoft is warning organizations about the risks associated with the discontinued Boa web server after vulnerabilities affecting the software were apparently exploited by threat actors in an operation aimed at the energy sector.

In 2021, threat intelligence company Recorded Future reported seeing a Chinese threat group targeting operational assets within India's power grid. In April 2022, the cybersecurity firm published a new report describing attacks launched by a different Chinese state-sponsored threat actor against organizations in India's power sector.

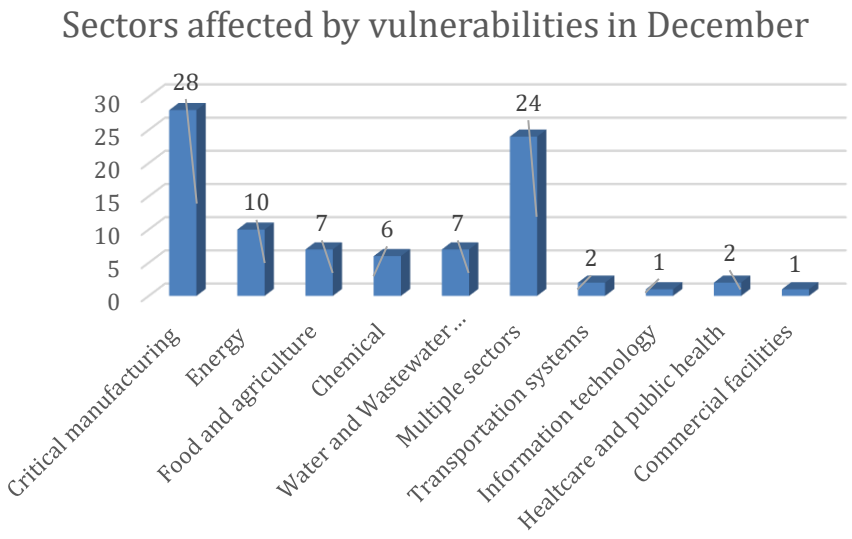
Targets included several State Load Despatch Centres (SLDCs) responsible for carrying out grid control and electricity dispatch operations. These SLDCs maintain grid frequency and stability through access to supervisory control and data acquisition (SCADA) systems. …

Source and more information:

https://www.securityweek.com/microsoft-warns-boa-web-server-risks-after-hackers-target-it-power-grid-attacks

ICS vulnerabilities

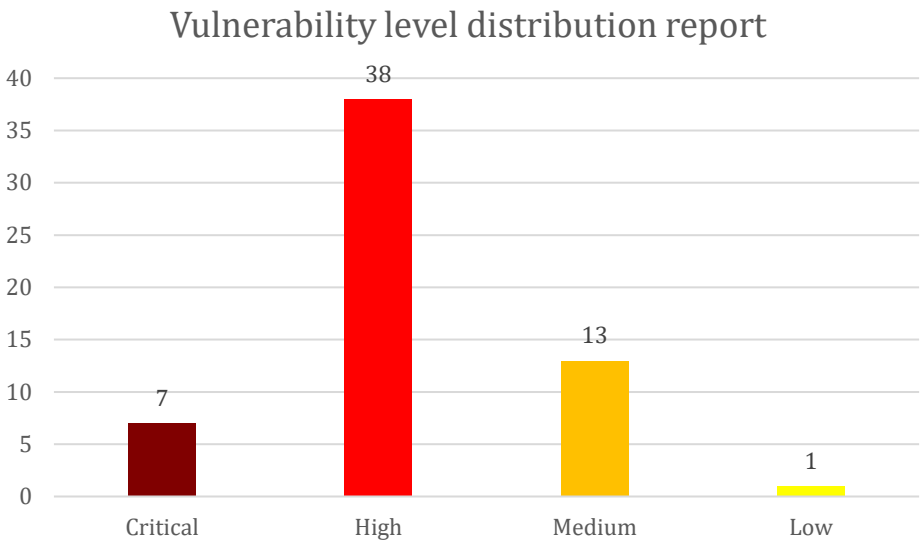
In December 2022, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:



Average number of vulnerabilities per vulnerability report in December: **2,08**

The most common vulnerabilities in December:

Vulnerability	CWE number	Items
Uncontrolled Resource Consumption	CWE-400	7
Improper Input Validation	CWE-20	6
Improper Access Control	CWE-284	5
Out-of-bounds Write	CWE-787	5
Use After Free	CWE-416	4
Out-of-bounds Read	CWE-125	4



ICSA-22-356-01: **Priva TopControl Suite**

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

Priva TopControl Suite | CISA

ICSA-22-356-02: **Rockwell Automation Studio 5000 Logix Emulate**

High level vulnerability: Improper Access Control.

Rockwell Automation Studio 5000 Logix Emulate | CISA

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

High level vulnerability: Improper Resource Shutdown or Release.

Mitsubishi Electric MELSEC iQ-R, iQ-L Series and MELIPC Series | CISA

ICSA-22-356-04: **Omron CX-Programmer**

High level vulnerability: Out-of-bounds Write.

Omron CX-Programmer | CISA

ICSA-22-354-01: **Fuji Electric Tellus Lite V-Simulator**

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

Fuji Electric Tellus Lite V-Simulator | CISA

ICSA-22-354-02: **Rockwell Automation GuardLogix and ControlLogix controllers**

High level vulnerability: Improper Input Validation.

Rockwell Automation GuardLogix and ControlLogix controllers | CISA

ICSA-22-354-03: **ARC Informatique PcVue**

Medium level vulnerabilities: Cleartext Storage of Sensitive Information, Insertion of Sensitive Information into Log File.

ARC Informatique PcVue | CISA

ICSA-22-354-04: **Rockwell Automation MicroLogix 1100 and 1400**

High level vulnerabilities: Cross-site Scripting, Improper Restriction of Rendered UI Layers or Frames.

Rockwell Automation MicroLogix 1100 and 1400 | CISA

ICSA-22-354-05: **Delta 4G Router DX-3021**

High level vulnerability: Command Injection.

Delta 4G Router DX-3021 | CISA

ICSA-22-349-01: **Prosys OPC UA Simulation Server**

Medium level vulnerability: Insufficiently Protected Credentials.

Prosys OPC UA Simulation Server | CISA

ICSA-22-349-02: **Siemens SCALANCE X-200RNA Switch Devices**

High level vulnerabilities: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS), Uncontrolled Resource Consumption, Use of Insufficiently Random Values, Improper Access Control, Exposure of Sensitive Information to an Unauthorized Actor.

Siemens SCALANCE X-200RNA Switch Devices | CISA

ICSA-22-349-03: **Siemens Multiple Denial of Service Vulnerabilities in Industrial Products**

High level vulnerabilities: Improper Input Validation, Improper Validation of Specified Quantity in Input, Improper Validation of Specified Type of Input, Improper Validation of Syntactic Correctness of Input.

Siemens Multiple Denial of Service Vulnerabilities in Industrial Products | CISA

ICSA-22-349-04: **Siemens Multiple Vulnerabilities in SCALANCE Products**

High level vulnerabilities: Code Injection, Use of a Broken or Risky Cryptographic Algorithm, Storing Passwords in a Recoverable Format, Improper Validation of Specified Quantity in Input, Improper Control of a Resource Through its Lifetime.

Siemens Multiple Vulnerabilities in SCALANCE Products | CISA

ICSA-22-346-05: **Siemens PLM Help Server**

Medium level vulnerability: Cross-site Scripting.

Siemens PLM Help Server | CISA

ICSA-22-349-06: **Siemens SIMATIC WinCC OA Ultralight Client**

Medium level vulnerability: Argument Injection.

Siemens SIMATIC WinCC OA Ultralight Client | CISA

ICSA-22-349-07: **Siemens Simcenter STAR-CCM+**

High level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens Simcenter STAR-CCM+ | CISA

ICSA-22-349-08: **Siemens Polarion ALM**

Medium level vulnerability: Injection.

Siemens Polarion ALM | CISA

ICSA-22-349-09: **Siemens Products affected by OpenSSL 3.0**

High level vulnerability: Classic Buffer Overflow.

Siemens Products affected by OpenSSL 3.0 | CISA

ICSA-22-349-10: **Siemens APOGEE/TALON Field Panels**

Medium level vulnerability: Predictable Exact Value from Previous Values.

Siemens APOGEE/TALON Field Panels | CISA

ICSA-22-349-11: **Siemens SIPROTEC 5 Devices**

Medium level vulnerability: Uncontrolled Resource Consumption.

Siemens SIPROTEC 5 Devices | CISA

ICSA-22-349-12: **Siemens Parasolid**

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

Siemens Parasolid | CISA

ICSA-22-349-13: **Siemens Mendix Workflow Commons**

High level vulnerability: Improper Access Control.

Siemens Mendix Workflow Commons | CISA

ICSA-22-349-14: **Siemens SISCO MMS-EASE Third Party Component**

High level vulnerability: Resource Management Errors.

Siemens SISCO MMS-EASE Third Party Component | CISA

ICSA-22-349-15: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-22-349-16: **Siemens APOGEE and TALON**

High level vulnerability: Improper Access Control.

Siemens APOGEE and TALON | CISA

ICSA-22-349-17: **Siemens Mendix Email Connector**

High level vulnerability: Improper Access Control.

Siemens Mendix Email Connector | CISA

ICSA-22-349-18: **Siemens SCALANCE SC-600 Family**

High level vulnerabilities: Out-of-bounds Write, Use After Free, Allocation of Resources Without Limits or Throttling.

Siemens SCALANCE SC-600 Family | CISA

ICSA-22-349-19: **Siemens SICAM PAS**

High level vulnerabilities: Uncontrolled Search Path Element, Improper Validation of Specified Type of Input, Cleartext Transmission of Sensitive Information.

Siemens SICAM PAS | CISA

ICSA-22-349-20: **Siemens Teamcenter Visualization and JT2Go**

High level vulnerabilities: NULL Pointer Dereference, Out-of-bounds Write, Out-of-bounds Read, Use After Free, Divide by Zero, Allocation of Resources Without Limits or Throttling.

Siemens Teamcenter Visualization and JT2Go | CISA

ICSA-22-349-21: **Siemens SCALANCE X-200RNA Switch Devices**

Critical level vulnerabilities: Observable Timing Discrepancy; Race Condition; Improper Restriction of Operations within the Bounds of a Memory Buffer; Improper Input Validation; NULL Pointer Dereference; Use After Free; Cryptographic Issues; Comparison of Incompatible Types; Resource Management Errors; Incorrect Calculation; Exposure of Sensitive Information to an Unauthorized Actor; Permissions, Privileges, and Access Controls; Out-of-bounds Write; Improper Authentication; Integer Overflow or Wraparound; Observable Discrepancy; Out-of-bounds Read; Missing Release of Memory after Effective Lifetime; Uncontrolled Resource Consumption; Untrusted Search Path; Incorrect Permission Assignment for Critical Resource; Incorrect Authorization; Improper Certificate Validation; Improper Encoding or Escaping of Output; Inappropriate Encoding for Output Context; Path Traversal.

Siemens SCALANCE X-200RNA Switch Devices | CISA

ICSA-21-012-02: **Siemens SCALANCE X Switches (Update C)**

Critical level vulnerability: Use of Hard-coded Cryptographic Key.

Siemens SCALANCE X Switches (Update C) | CISA

ICSA-20-014-03: **Siemens SCALANCE X Switches (Update B)**

High level vulnerability: Missing Authentication for Critical Function.

Siemens SCALANCE X Switches (Update B) | CISA

ICSA-20-042-07: **Siemens SCALANCE X Switches (Update C)**

Low level vulnerability: Protection Mechanism Failure.

Siemens SCALANCE X Switches (Update C) | CISA

ICSA-22-069-01: **Siemens RUGGEDCOM Devices (Update D)**

Medium level vulnerability: Inadequate Encryption Strength.

Siemens RUGGEDCOM Devices (Update D) | CISA

ICSA-21-222-05: **Siemens Industrial Products Intel CPUs (Update G)**

High level vulnerability: Missing Encryption of Sensitive Data.

Siemens Industrial Products Intel CPUs (Update G) | CISA

ICSA-20-161-04: **Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update K)**

High level vulnerability: Unquoted Search Path or Element.

Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Update K) | CISA

ICSA-22-286-09: **Siemens SICAM P850 and P855 Devices (Update A)**

Critical level vulnerabilities: Session Fixation, Improper Neutralization of Parameter/Argument Delimiters.

Siemens SICAM P850 and P855 Devices (Update A) | CISA

ICSA-22-286-11: **Siemens SCALANCE and RUGGEDCOM Products (Update B)**

High level vulnerability: Missing Authorization.

Siemens SCALANCE and RUGGEDCOM Products (Update B) | CISA

ICSA-22-258-04: **Siemens Mendix SAML Module (Update B)**

High level vulnerability: Authentication Bypass by Capture-replay.

Siemens Mendix SAML Module (Update B) | CISA

ICSA-22-104-06: **Siemens PROFINET Stack Integrated on Interniche Stack (Update E)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

Siemens PROFINET Stack Integrated on Interniche Stack (Update E) | CISA

ICSA-22-286-07: **Siemens Nucleus RTOS FTP Server (Update A)**

High level vulnerability: Uncontrolled Resource Consumption.

Siemens Nucleus RTOS FTP Server (Update A) | CISA

ICSA-22-314-09: **Siemens Teamcenter Visualization and JT2Go (Update A)**

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

Siemens Teamcenter Visualization and JT2Go (Update A) | CISA

ICSA-22-314-02: **Siemens Web Server Login Page of Industrial Controllers (Update A)** **Medium** level vulnerability: Cross-Site Request Forgery (CSRF).

Siemens Web Server Login Page of Industrial Controllers (Update A) | CISA

ICSA-22-167-14: **Siemens OpenSSL Affected Industrial Products (Update E)**

High level vulnerability: Infinite Loop.

Siemens OpenSSL Affected Industrial Products (Update E) | CISA

ICSA-22-132-05: **Siemens Industrial PCs and CNC devices (Update A)**

High level vulnerabilities: Improper Input Validation, Improper Authentication, Improper Isolation of Shared Resources on System-on-a-Chip, Improper Privilege Management.

Siemens Industrial PCs and CNC devices (Update A) | CISA

ICSA-22-104-13: **Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem (Update A)** **Critical** level vulnerability: Use of Unmaintained Third-party Components.

Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem (Update A) | CISA

ICSA-18-163-02: **Siemens SCALANCE X Switches (Update B)**

Medium level vulnerability: Cross-site Scripting.

Siemens SCALANCE X Switches (Update B) | CISA

ICSA-22-132-12: **Siemens Industrial Products (Update C)**

High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Industrial Products (Update C) | CISA

ICSA-20-105-08: **Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update D)**

High level vulnerability: Uncontrolled Resource Consumption.

Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update D) | CISA

ICSA-19-283-02: **Siemens PROFINET Devices (Update L)**

High level vulnerability: Uncontrolled Resource Consumption.

Siemens PROFINET Devices (Update L) | CISA

ICSA-22-347-01: **ICONICS and Mitsubishi Electric Products**

Medium level vulnerability: Path Traversal.

ICONICS and Mitsubishi Electric Products | CISA

ICSA-22-347-02: **Schneider Electric APC Easy UPS Online**

Critical level vulnerabilities: Missing Authentication for Critical Function, Unrestricted Upload of File with Dangerous Type, Incorrect Permission Assignment for Critical Resource, Use of Hard-coded Credentials.

Schneider Electric APC Easy UPS Online | CISA

ICSA-22-347-03: **Contec CONPROSSYS HMI System (CHS)**

Critical level vulnerability: OS Command Injection.

Contec CONPROSSYS HMI System (CHS) | CISA

ICSA-22-342-01: **Advantech iView**

High level vulnerability: SQL Injection.

Advantech iView | CISA

ICSA-22-342-02: **AVEVA InTouch Access Anywhere**

High level vulnerability: Relative Path Traversal.

AVEVA InTouch Access Anywhere | CISA

ICSA-22-342-03: **Rockwell Automation Logix controllers**

High level vulnerability: Improper Input Validation.

Rockwell Automation Logix controllers | CISA

ICSMA-22-335-01: **BD BodyGuard Pumps**

Medium level vulnerability: Missing Protection Mechanism for Alternate Hardware Interface.

BD BodyGuard Pumps | CISA

ICSA-22-335-01: **Mitsubishi Electric MELSEC iQ-R Series**

High level vulnerability: Improper Input Validation.

Mitsubishi Electric MELSEC iQ-R Series | CISA

ICSA-22-335-02: **Horner Automation Remote Compact Controller**

Critical level vulnerabilities: Inadequate Encryption Strength, Use of Hard-coded Cryptographic Key, Excessive Reliance on Global Variables.

Horner Automation Remote Compact Controller | CISA

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

https://ics-cert.us-cert.gov/advisories

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

In December 2022, ICS-CERT has published an alert.

#StopRansomware: Cuba Ransomware

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Cuba ransomware IOCs and TTPs associated with Cuba ransomware actors identified through FBI investigations, third-party reporting, and open-source reporting. This advisory updates the December 2021 FBI Flash: Indicators of Compromise Associated with Cuba Ransomware.

Note: While this ransomware is known by industry as "Cuba ransomware," there is no indication Cuba ransomware actors have any connection or affiliation with the Republic of Cuba.

Since the release of the December 2021 FBI Flash, the number of U.S. entities compromised by Cuba ransomware has doubled, with ransoms demanded and paid on the increase.

This year, Cuba ransomware actors have added to their TTPs, and third-party and open-source reports have identified a possible link between Cuba ransomware actors, RomCom Remote Access Trojan (RAT) actors, and Industrial Spy ransomware actors.

FBI and CISA encourage organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of Cuba ransomware and other ransomware operations.

Five critical infrastructure sectors affected: Financial Services, Government Facilities, Healthcare and Public Health, Critical Manufacturing, and Information Technology.

More information and the IoC's available on the following link:

https://www.cisa.gov/uscert/ncas/alerts/aa22-335a