2024 September, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, podcasts, 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

Singapore's Operational Technology Cybersecurity Masterplan 2024

Singapore's Operational Technology (OT) Cybersecurity Masterplan ("Masterplan") represents ongoing commitment to bolstering the security and resilience of organizations that operate industrial control systems and utilize OT technologies for physical control functions. The 2024 edition of the Masterplan has been updated to reflect the growing maturity of the OT ecosystem and the increasingly complex cyber threats facing OT systems due to geopolitical and technological developments.

The Masterplan 2024 was developed collaboratively with the OT community, involving over 60 organizations, including consulting and professional services firms, Institutes of Higher Learning and training providers, Critical Information Infrastructure (CII) operators, relevant government bodies, OT Original Equipment Manufacturers (OEMs), system integrators, cybersecurity solution providers, cloud service providers, and OT Small and Medium-Sized Enterprises (SMEs).

In the updated Masterplan, the Cyber Security Agency (CSA) will advocate for the adoption of Secure-by-Deployment principles to ensure the security of OT systems throughout their entire lifecycle, from product design and deployment to maintenance, engaging multiple stakeholders.

The Masterplan contains the followings:

1. Enhance the OT Cybersecurity Talent Pipeline
2. Enhance Information Sharing and Reporting
3. Uplift OT Cybersecurity Resilience beyond CII
4. Establish an OT Cybersecurity Centre of Excellence and promote Secure-By-Deployment throughout the lifecycle of the OT systems

Source, links (where you can download the Masterplan) and more information available on the following link:

https://www.csa.gov.sg/Tips-Resource/publications/2024/operational-technology-cybersecurity-masterplan-2024

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in October 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 October 2024, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

ICS Cybersecurity Conference

SecurityWeek's Industrial Control Systems (ICS) Cybersecurity Conference is the largest and longest-running event series focused on industrial cybersecurity. Since 2002, the conference has gathered ICS cyber security stakeholders across various industries and attracts operations and control engineers, IT, government, vendors and academics.

Atlanta, GA, USA; 21st – 24th October 2024

More details can be found on the following website:

https://www.icscybersecurityconference.com/about-ics/

OT Cybersecurity Summit

The alarming rise in OT cyber-attacks on America's critical infrastructure has highlighted the urgent need to prioritize investment in defending against OT-specific cyber threats. Oil and Gas, Utilities, and other critical infrastructure companies must reassess their approach to cybersecurity and mitigate attacks across converged systems. Investing in advanced threat detection, employee training to raise cyber risk awareness, and incident response capability has become more urgent than ever before.

Taking place in Houston, the OT Cybersecurity Summit will bring together OT, operations, ICS, SCADA and cybersecurity leaders to discuss how to reduce system vulnerabilities and cyber threats across your OT operating environment.

Houston, TX, USA; 28th – 29th October 2024

More details can be found on the following website:

https://www.oilandgasiq.com/events-otcybersecurity

11th Cyber & SCADA Security in Energy Sector 2024

This conference represents the pinnacle of Energy Sector Security Excellence, offering an immersive exploration into safeguarding critical infrastructure against evolving cyber threats.

In an era where digital technologies seamlessly integrate into power and utility systems, ensuring robust cybersecurity measures is not just important but imperative. The summit is meticulously crafted to empower cybersecurity professionals, SCADA engineers, and utility executives, providing them with the essential knowledge and tools to successfully navigate these evolving challenges.

Amsterdam, Netherlands; 28th – 29th October 2024

More details can be found on the following website:

https://cyber-scada-power-utilities.com/

ICS incidents

Stormous claims cyberattack on Belgian brewer

On March 6th, Duvel Moortgat brewery, a renowned Belgian beer producer, experienced a significant disruption as a result of a ransomware attack. The cyberattack, later claimed by the Stormous ransomware group, led to the immediate halt of production at the brewery. Alarms were triggered in the early hours, and the brewery's IT department quickly acted to contain the threat. According to spokesperson Ellen Aarts, the attack was detected early, but production had to be stopped indefinitely, with no exact timeline for resuming operations.

Despite the shutdown, Duvel reassured customers that there is no immediate shortage of beer. The brewery had sufficient stock to continue supplying its products, including its famous Duvel ale and other popular brands like Vedett and Maredsous. As of now, there are no updates on any ransom demands or whether the company plans to comply with them. However, the company remains focused on resolving the situation and restoring normal operations.

The incident sparked a humorous response from Belgian beer lovers, with comments on social media reflecting a lighthearted approach to the cyberattack. Some joked that the situation should be considered a national emergency, while others made light of the fact that brewery staff, apart from the IT department, were reportedly enjoying beers during the downtime.

At this stage, there is still uncertainty regarding when Duvel Moortgat will fully resume production, but the brewery remains hopeful of a swift recovery.

The source is available on the following link:

https://cybernews.com/news/duvel-moortgat-ransomware-attack/

Kansas water plant cyberattack forces switch to manual operations

Arkansas City, Kansas, had to switch its water treatment facility to manual operations due to a cyberattack detected at the end of the month. City officials, alongside Homeland Security and the FBI, are investigating the breach. Despite the cyberattack, city manager Randy Frazer reassured residents that the water supply remains safe and has not been compromised. The manual operations are a precaution while authorities work on resolving the issue.

The incident is part of a broader threat to U.S. water systems. Just days before the attack, the Water Information Sharing and Analysis Center (WaterISAC) warned of potential cyberattacks by Russian-linked groups targeting water utilities. The U.S. Environmental Protection Agency (EPA) also issued guidance to help water systems improve their cybersecurity defenses.

Cyberattacks on water systems are not new, with incidents attributed to Russian, Iranian, and Chinese groups in recent years. The U.S. water sector has been targeted by numerous cybercriminals, including ransomware attacks and breaches of critical infrastructure systems.

Enhanced security measures are currently in place, and city officials have noted some residents may experience low water pressure as technical issues are addressed. However, the water quality remains unaffected. The U.S. government continues to prioritize the defense of water systems from cyber threats, acknowledging the critical nature of these facilities to public health and safety.

The source is available on the following link:

https://www.bleepingcomputer.com/news/security/kansas-water-plant-cyberattack-forces-switch-to-manual-operations/

Book recommendation

OT Cybersecurity: twenty years after (IIOT)

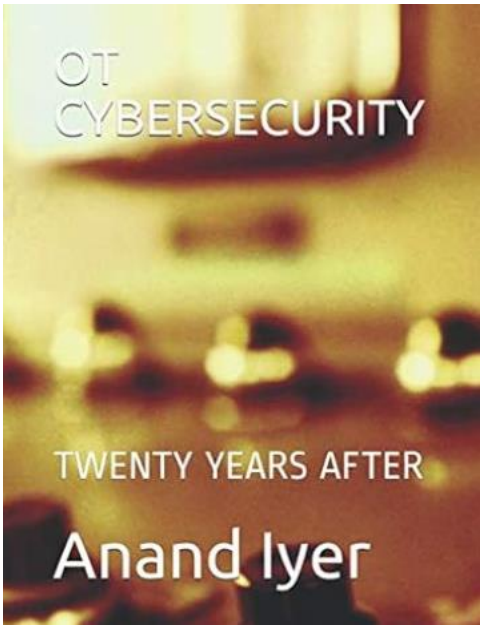
Twenty years ago, the author was asked to present a paper on protecting automation systems when connected to the net. This was probably one of the first attempts towards OT Cybersecurity. And 20 years later, the author looks at the landscape and tries to find some solutions to some problems that have remained problems since that day. In this book, the author provides some perspective on why some networks are the way they are (unauthenticated, unencrypted), looks at some problems like patching delays and looks at way forward towards resolving these sticky problems. The author also presents some innovative ideas to improve OT cybersecurity and workaround the old sticky problems. This book is a must for Industrial Automation, IIoT-Smart manufacturing, plant-factory operations professionals and Cybersecurity professionals. It is an economical quick guide to students pursuing OT cybersecurity. The book is written in a quick read format and users can fly through the concepts presented and those with time can also relish some incidents and the details of the concepts! Happy reading!

Author/Editor: Anand Iyer (Author)

Year of issue: 2020

The book is available at the following link:

https://www.amazon.com/OT-CYBERSECURITY-TWENTY-YEARS-AFTER/dp/B0882N6YNW



ICS security news selection

Halliburton Data Stolen in Oil-Sector Cyberattack

Halliburton has confirmed that data was stolen in the Aug. 21 cyberattack on its networks. The energy services company — which has a global presence in oil fields and runs some of the world's largest fracking operations — said in an 8K filing with the Securities and Exchange Commission today that "the company believes the unauthorized third party accessed and exfiltrated information from the company's systems.". ...

Source and more information:

https://www.darkreading.com/ics-ot-security/halliburton-data-stolen-oil-sector-attack

Michigan's EGLE rolls out cybersecurity strategy for water treatment operators

The Michigan Department of Environment, Great Lakes, and Energy (EGLE) highlighted on Tuesday its recent initiative to create a comprehensive preparedness strategy for drinking water and wastewater treatment plant operators in Michigan. The effort includes developing a robust cybersecurity preparedness and response plan for these operators. ...

Source and more information:

https://industrialcyber.co/utilities-energy-power-water-waste/michigans-egle-rolls-out-cybersecurity-strategy-for-water-treatment-operators/

Should ISA/IEC 62443 Security Level 1 Be the Minimum for safety instrumented systems (SIS)?

Safety instrumented systems (SIS) are playing a vital role to keep plants run in a safe manner to prevent process parameters such as pressure, flow, level and temperature out of deviation and in safe operating levels, according to the design parameters of equipment and pipelines associated to the process. This article is about the importance of SIS and their regulation according to international standards.

Source and more information: https://industrialcyber.co/expert/should-isa-iec-62443-security-level-1-be-the-minimum-for-safety-instrumented-systems-sis/

Russian military hackers linked to critical infrastructure attacks

The United States and its allies have linked a group of Russian hackers (tracked as Cadet Blizzard and Ember Bear) behind global critical infrastructure attacks to Unit 29155 of Russia's Main Directorate of the General Staff of the Armed Forces (also known as GRU).

In a joint advisory published today, the Russian GRU military intelligence hackers, known for deploying WhisperGate data-wiping malware in Ukraine in January 2022, are described as "junior active-duty GRU officers" part of GRU's 161st Specialist Training Center and coordinated by experienced Unit 29155 leadership. ...

Source and more information:

https://www.bleepingcomputer.com/news/security/us-and-allies-link-russian-military-hackers-behind-critical-infrastructure-attacks-to-gru-unit-29155/

SANS Institute highlights urgent need for enhanced ICS/OT security amid rising cyber threats

The SANS Institute explored in a recent document the vital role of ICS (industrial control systems) in critical infrastructure, examines the ICS/OT (operational technology) threat landscape in 2024, while also defining why a robust and proactive approach to ICS/OT-specific security controls separate from IT security controls and processes is not just a technical necessity, but a fundamental business requirement. This comes as ICS and engineering operations, sophisticated facilities with engineering equipment, and specialized software that control, monitor, and drive physical industrial processes in critical infrastructure sectors, make these critical installations an attractive target for malicious adversaries. ...

Source and more information:

https://industrialcyber.co/control-device-security/sans-institute-highlights-urgent-need-for-enhanced-ics-ot-security-amid-rising-cyber-threats/

Air-Gapped Networks Vulnerable to Acoustic Attack via LCD Screens

In the "PixHell" attack, sound waves generated by pixels on a screen can transmit information across seemingly impenetrable air gaps.

A newly devised covert channel attack method could undermine diligently devised air gaps at highly sensitive organizations.

In industrial control systems security, the term "air gap" is contested. It typically describes a total physical separation between networks — a literal gap through which no Wi-Fi signals, wires, etc., can pass. The most critical military, government, and industrial sites use air gaps to prevent Internet-based cyber threats from penetrating the kinds of networks that protect state secrets and human lives. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/air-gapped-networks-vulnerable-to-acoustic-attack-via-lcd-screens

Remote Access Sprawl Strains Industrial OT Network Security

A veritable grab bag of tools used to access critical infrastructure networks are wildly insecure, and they're blobbing together to create a widening attack surface.

The exploding demand for remote access into today's industrial control systems (ICS) and operational technology (OT) systems has created a nebulous, Internet-connected attack surface that's too attractive for cyberattackers to ignore. And cleanup is not going to be a simple affair.

Far too many ICS networks are being accessed by employees, partners, suppliers, and customers using a slapped-together mousetrap of tools, leaving these environments woefully exposed while connected to the Internet, according to researchers. ...

Source and more information:

https://www.darkreading.com/ics-ot-security/remote-access-sprawl-industrial-ot-network-security

Achieving IT-OT integration emerges as critical step for industrial efficiency and security

Integrating IT and OT environments has become a critical aspect of the modern, fast-changing industrial world, supporting the drive for business goals and bolstering OT cyberinfrastructure. The move unites the digital and physical worlds, providing opportunities for organizations to optimize their operation and ultimately become more efficient and secure. IT-OT integration also helps ensure that organizational goals across these environments align to enable businesses to make informed decisions based on real-time data analytics, streamline processes, and reduce downtime.

Productivity will benefit from predictive maintenance, identifying potential issues ahead of their probable escalation, and minimizing operational disruptions of critical assets. …

Source and more information:

https://industrialcyber.co/features/achieving-it-ot-integration-emerges-as-critical-step-for-industrial-efficiency-and-security/

Need to strengthen governance and compliance measures to bolster OT cybersecurity and ICS protection

Governance and compliance are crucial when it comes to OT (operational technology) cybersecurity in protecting ICS (industrial control systems) from an increasingly growing threat landscape. These developments are bringing cybersecurity forward from computers and control systems into the Internet-connected field devices. All of this means that the higher the level of sophistication involved in cyber threats, the further the governance framework evolves in countering them through strict policies, risk management, and continued monitoring. …

Source and more information:

https://industrialcyber.co/features/need-to-strengthen-governance-and-compliance-measures-to-bolster-ot-cybersecurity-and-ics-protection/

Israeli Group Claims Lebanon Water Hack as CISA Reiterates Warning on Simple ICS Attacks

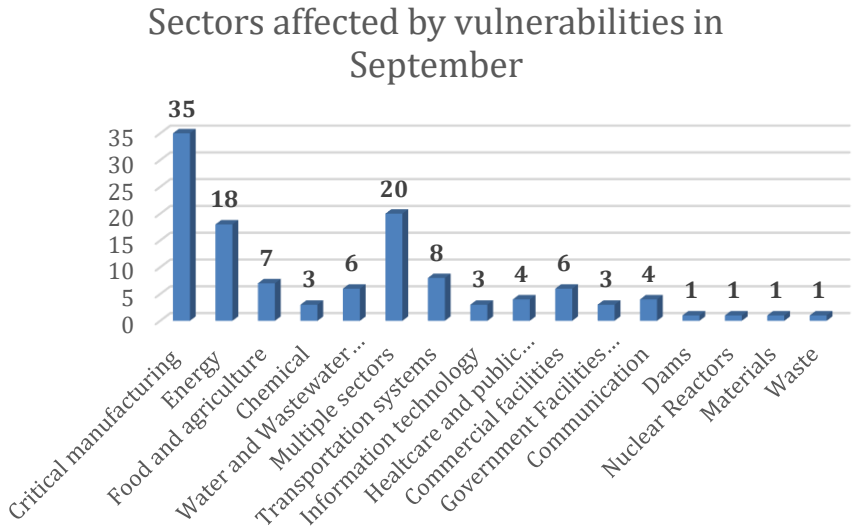
The US cybersecurity agency CISA on Wednesday reiterated a warning that unsophisticated methods can be used to hack industrial control systems (ICS) and other operational technology (OT). Even so, some threat actors appear to be making exaggerated claims when it comes to attacks on such systems. …

Source and more information:

https://www.securityweek.com/israeli-group-claims-lebanon-water-hack-as-cisa-reiterates-warning-on-simple-ics-attacks/

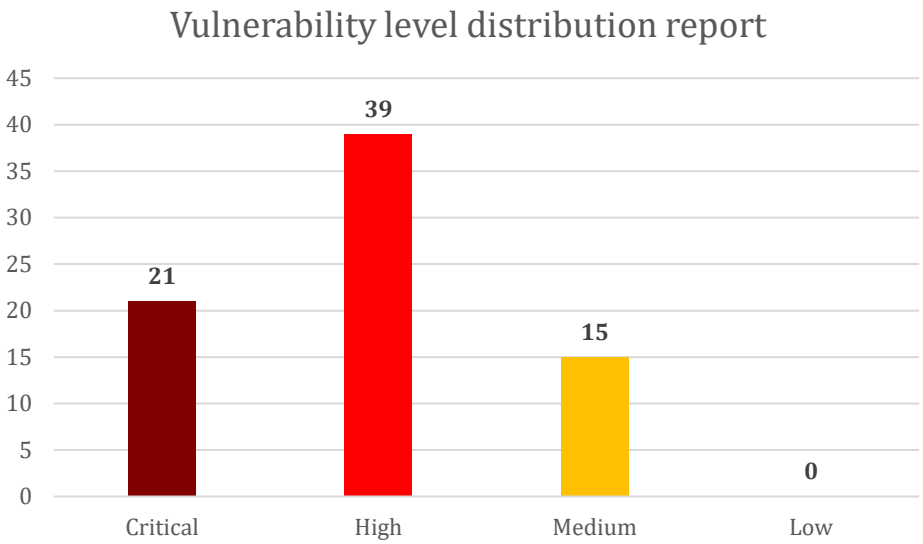
ICS vulnerabilities

In September 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 September:

Vulnerability	CWE number	Items
Improper Input Validation	CWE-20	9
Cross-site Scripting	CWE-79	6
Missing Authentication for Critical Function	CWE-306	5
Cleartext Transmission of Sensitive Information	CWE-319	5
Improper Access Control	CWE-284	5
Command injection	CWE-77	4
Observable Response Discrepancy	CWE-204	4
Uncontrolled Resource Consumption	CWE-400	4



IICSA-24-270-01: **Advantech ADAM-5550**

High level vulnerabilities: Weak Encoding for Password, Cross-site Scripting.

Advantech ADAM-5550 | CISA

ICSA-24-270-02: **Advantech ADAM-5630**

High level vulnerabilities: Use of Persistent Cookies Containing Sensitive Information, Cross-site request forgery (CSRF), Weak Encoding for Password, Missing Authentication for Critical Function.

Advantech ADAM-5630 | CISA

ICSA-24-270-03: **Atelmo Atemio AM 520 HD Full HD Satellite Receiver**

Critical level vulnerability: OS Command Injection.

Atelmo Atemio AM 520 HD Full HD Satellite Receiver | CISA

ICSA-24-270-04: **goTenna Pro X and Pro X2**

High level vulnerabilities: Weak Password Requirements, Insecure Storage of Sensitive Information, Missing Support for Integrity Check, Cleartext Transmission of Sensitive Information, Improper Restriction of Communication Channel to Intended Endpoints, Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Weak Authentication, Insertion of Sensitive Information Into Sent Data, Observable Response Discrepancy, Missing Authentication for Critical Function.

goTenna Pro X and Pro X2 | CISA

ICSA-24-270-05: **goTenna Pro ATAK Plugin**

High level vulnerabilities: Weak Password Requirements, Insecure Storage of Sensitive Information, Missing Support for Integrity Check, Cleartext Transmission of Sensitive Information, Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Weak Authentication, Insertion of Sensitive Information Into Sent Data, Observable Response Discrepancy, Insertion of Sensitive Information Into Sent Data.

goTenna Pro ATAK Plugin | CISA

ICSA-24-268-01: **OPW Fuel Management Systems SiteSentinel**

Critical level vulnerability: Missing Authentication For Critical Function.

OPW Fuel Management Systems SiteSentinel | CISA

ICSA-24-268-02: **Alisonic Sibylla**

Critical level vulnerability: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Alisonic Sibylla | CISA

ICSA-24-268-03: **Franklin Fueling Systems TS-550 EVO**

High level vulnerability: Absolute Path Traversal.

Franklin Fueling Systems TS-550 EVO | CISA

ICSA-24-268-04: **Dover Fueling Solutions ProGauge MAGLINK LX CONSOLE**

Critical level vulnerabilities: Command Injection, Improper Privilege Management, Use of Hard-coded Password, Cross-site Scripting, Authentication Bypass Using an Alternate Path or Channel.

Dover Fueling Solutions ProGauge MAGLINK LX CONSOLE | CISA

ICSA-24-268-05: **Moxa MXview One**

Medium level vulnerabilities: Cleartext Storage In A File or On Disk, Path Traversal, Time-of-Check Time-of-Use Race Condition.

Moxa MXview One | CISA

ICSA-24-268-06: **OMNTEC Proteus Tank Monitoring**

Critical level vulnerability: Missing Authentication for Critical Function.

OMNTEC Proteus Tank Monitoring | CISA

ICSA-24-156-01: **Uniview NVR301-04S2-P4 (Update A)**

Medium level vulnerability: Cross-site Scripting.

Uniview NVR301-04S2-P4 (Update A) | CISA

ICSA-19-274-01: **Interpeak IPnet TCP/IP Stack (Update E)**

Critical level vulnerabilities: Stack-based Buffer Overflow, Heap-based Buffer Overflow, Integer Underflow (Wrap or Wraparound), Improper Restriction of Operations within the Bounds of a Memory Buffer, Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), NULL Pointer Dereference.

Interpeak IPnet TCP/IP Stack (Update E) | CISA

ICSA-24-263-01: **Rockwell Automation RSLogix 5 and RSLogix 500**

High level vulnerability: Insufficient verification of data authenticity.

Rockwell Automation RSLogix 5 and RSLogix 500 | CISA

ICSA-24-263-02: **IDEC PLCs**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Generation of Predictable Identifiers.

IDEC PLCs | CISA

ICSA-24-263-03: **IDEC CORPORATION WindLDR and WindO/I-NV4**

Medium level vulnerability: Cleartext Storage of Sensitive Information.

IDEC CORPORATION WindLDR and WindO/I-NV4 | CISA

ICSA-24-263-04: **MegaSys Computer Technologies Telenium Online Web Application**

Critical level vulnerability: Improper Input Validation.

MegaSys Computer Technologies Telenium Online Web Application | CISA

ICSA-24-263-05: **Kastle Systems Access Control System**

Critical level vulnerabilities: Use of Hard-coded Credentials, Cleartext Storage of Sensitive Information.

Kastle Systems Access Control System | CISA

ICSA-24-261-01: **Siemens SIMATIC S7-200 SMART Devices**

High level vulnerability: Uncontrolled Resource Consumption.

Siemens SIMATIC S7-200 SMART Devices | CISA

ICSA-24-261-02: **Millbeck Communications Proroute H685t-w**

High level vulnerabilities: Command Injection, Cross-site Scripting.

Millbeck Communications Proroute H685t-w | CISA

ICSA-24-261-03: **Yokogawa Dual-redundant Platform for Computer (PC2CKM)**

High level vulnerability: Unchecked Return Value.

Yokogawa Dual-redundant Platform for Computer (PC2CKM) | CISA

SSA-097435: **Siemens Mendix Runtime (Update: 1.1.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435 (siemens.com)

SSA-999588: **Siemens User Management Component (UMC) Before V2.11.2 (Update: 1.5.)**

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-962515: **Siemens Industrial Products (Update: 1.2.)**

High level vulnerability: Out-of-bounds Read.

SSA-962515 (siemens.com)

SSA-955858: **Siemens LOGO! 8 BM Devices (Update: 1.2.)**

Critical level vulnerabilities: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), Improper Input Validation, Improper Validation of Specified Index, Position, or Offset in Input.

SSA-955858 (siemens.com)

SSA-921449: **Siemens LOGO! V8.3 BM Devices (Update: 1.1.)**

Medium level vulnerability: Plaintext Storage of a Password.

SSA-921449 (siemens.com)

SSA-883918: **Siemens SIMATIC WinCC (Update: 1.1.)**

High level vulnerability: Exposure of Private Personal Information to an Unauthorized Actor.

SSA-883918 (siemens.com)

SSA-844582: **Siemens LOGO! V8.3 BM Devices Results in Broken LOGO! V8.3 Product CA (Update: 1.1.)**

High level vulnerability: Improper Protection against Electromagnetic Fault Injection (EM-FI).

SSA-844582 (siemens.com)

SSA-832273: **Fortigate NGFW Before V7.4.3 on Siemens RUGGEDCOM APE1808 Devices (Update: 1.5.)**

High level vulnerabilities: Multiple.

SSA-832273 (siemens.com)

SSA-792319: **Siemens SENTRON 7KM PAC3x20 Devices (Update: 1.1.)**

Medium level vulnerability: Improper Access Control.

SSA-792319 (siemens.com)

SSA-783481: **Siemens LOGO! 8 BM (Update: 1.2.)**

Medium level vulnerability: Improper Handling of Exceptional Conditions.

SSA-783481 (siemens.com)

SSA-753746: **Siemens SIMATIC WinCC Affecting Other SIMATIC Software Products (Update: 1.4.)**

High level vulnerability: NULL Pointer Dereference.

SSA-753746 (siemens.com)

SSA-698820: **Fortigate NGFW on Siemens RUGGEDCOM APE1808 Devices (Update: 1.2.)**

High level vulnerabilities: Stack-based Buffer Overflow, Use of Password Hash With Insufficient Computational Effort, Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incorrect Parsing of Numbers with Different Radices, Improper Access Control.

SSA-698820 (siemens.com)

SSA-691715: **OPC Foundation Local Discovery Server Affecting Siemens Products (Update: 1.6.)**

High level vulnerability: Improper Input Validation.

SSA-691715 (siemens.com)

SSA-690517: **Siemens SCALANCE W700 802.11 AX Family (Update: 1.1.)**

High level vulnerabilities: Improper Control of a Resource Through its Lifetime, Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Hard-coded Cryptographic Key, Use of Weak Hash, Unsynchronized Access to Shared Data in a Multithreaded Context.

SSA-690517 (siemens.com)

SSA-566905: **Webserver of Siemens Industrial Products (Update: 1.3.)**

High level vulnerabilities: Use After Free, Deadlock, Allocation of Resources Without Limits or Throttling.

SSA-566905 (siemens.com)

SSA-455250: **Palo Alto Networks Virtual NGFW on Siemens RUGGEDCOM APE1808 Devices Before V11.1.2-h3 (Update: 1.3.)**

Critical level vulnerabilities: Multiple.

SSA-455250 (siemens.com)

SSA-349422: **Siemens Industrial Real-Time (IRT) Devices (Update: 2.1.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-349422 (siemens.com)

SSA-293562: **Siemens PROFINET DCP Implementation of Industrial Products (Update: 3.6.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-293562 (siemens.com)

SSA-280603: **Siemens SINUMERIK ONE and SINUMERIK MC (Update: 1.1.)**

High level vulnerability: Use After Free.

SSA-280603 (siemens.com)

SSA-088132: **OPC UA Server Implementations of Several Siemens Industrial Products (Update: 1.1.)**

Medium level vulnerability: Improperly Controlled Sequential Memory Allocation.

SSA-088132 (siemens.com)

ICSA-24-256-01: **Siemens SINEMA Remote Connect Server**

Medium level vulnerability: Session Fixation.

Siemens SINEMA Remote Connect Server | CISA

ICSA-24-256-02: **Siemens SINUMERIK ONE, SINUMERIK 840D and SINUMERIK 828D Critical** level vulnerability: Incorrect Permission Assignment for Critical Resource.

Siemens SINUMERIK ONE, SINUMERIK 840D and SINUMERIK 828D | CISA

ICSA-24-256-03: **Siemens User Management Component (UMC)**

Critical level vulnerability: Heap-based Buffer Overflow.

Siemens User Management Component (UMC) | CISA

ICSA-24-256-04: **Siemens SINUMERIK Systems**

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

Siemens SINUMERIK Systems | CISA

ICSA-24-256-05: **Siemens Mendix Runtime**

Medium level vulnerability: Observable Response Discrepancy.

Siemens Mendix Runtime | CISA

ICSA-24-256-06: **Siemens Automation License Manager**

Critical level vulnerability: Integer Overflow or Wraparound.

Siemens Automation License Manager | CISA

ICSA-24-256-07: **Siemens SIMATIC RFID Readers**

High level vulnerabilities: Hidden Functionality, Exposure of Sensitive Information to an Unauthorized Actor, Improper Check or Handling of Exceptional Conditions, Improper Access Control.

Siemens SIMATIC RFID Readers | CISA

ICSA-24-256-08: **Siemens Industrial Products**

Medium level vulnerability: Improper Input Validation.

Siemens Industrial Products | CISA

ICSA-24-256-09: **Siemens SIMATIC, SIPLUS, and TIM**

High level vulnerability: NULL Pointer Dereference.

Siemens SIMATIC, SIPLUS, and TIM | CISA

ICSA-24-256-10: **Siemens SINEMA**

Medium level vulnerabilities: Use After Free, Improper Input Validation, Improper Certificate Validation, Missing Release of Resource after Effective Lifetime, Improper Validation of Certificate with Host Mismatch, Insufficient Session Expiration, Insertion of Sensitive Information into Log File.

Siemens SINEMA | CISA

ICSA-24-256-11: **Siemens Industrial Edge Management**

Critical level vulnerability: Authorization Bypass Through User-Controlled Key.

Siemens Industrial Edge Management | CISA

ICSA-24-256-12: **Siemens Tecnomatix Plant Simulation**

High level vulnerability: Stack-based Buffer Overflow.

Siemens Tecnomatix Plant Simulation | CISA

ICSA-24-256-13: **Siemens SCALANCE W700**

Critical level vulnerability: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection').

Siemens SCALANCE W700 | CISA

ICSA-24-256-14: **Siemens SIMATIC SCADA and PCS 7 Systems**

Critical level vulnerability: Execution with Unnecessary Privileges.

Siemens SIMATIC SCADA and PCS 7 Systems | CISA

ICSA-24-256-15: **Siemens Industrial Products**

High level vulnerability: Signal Handler Race Condition.

Siemens Industrial Products | CISA

ICSA-24-256-16: **Siemens Third Party Component in SICAM and SITIPE Products**

High level vulnerability: Classic Buffer Overflow.

Siemens Third Party Component in SICAM and SITIPE Products | CISA

ICSA-24-256-17: **AutomationDirect DirectLogic H2-DM1E**

High level vulnerabilities: Session Fixation, Authentication Bypass by Capture-replay.

AutomationDirect DirectLogic H2-DM1E | CISA

ICSA-24-256-18: **Rockwell Automation ControlLogix/GuardLogix 5580 and CompactLogix/Compact GuardLogix 5380**

High level vulnerability: Improper Input Validation.

Rockwell Automation ControlLogix/GuardLogix 5580 and CompactLogix/Compact GuardLogix 5380 | CISA

ICSA-24-256-19: **Rockwell Automation OptixPanel**

High level vulnerability: Improper Privilege Management.

Rockwell Automation OptixPanel | CISA

ICSA-24-256-20: **Rockwell Automation AADvance Trusted SIS Workstation**

High level vulnerabilities: Improper Input Validation, Out-Of-Bounds Write.

Rockwell Automation AADvance Trusted SIS Workstation | CISA

ICSA-24-256-21: **Rockwell Automation 5015-U8IHFT**

High level vulnerability: Improper Input Validation.

Rockwell Automation 5015-U8IHFT | CISA

ICSA-24-256-22: **Rockwell Automation FactoryTalk Batch View**

Critical level vulnerability: Improper Authentication.

Rockwell Automation FactoryTalk Batch View | CISA

ICSA-24-256-23: **Rockwell Automation FactoryTalk View Site**

Critical level vulnerability: Command Injection.

Rockwell Automation FactoryTalk View Site | CISA

ICSA-24-256-24: **Rockwell Automation Pavilion8**

High level vulnerabilities: Improper Privilege Management, Path Traversal.

Rockwell Automation Pavilion8 | CISA

ICSA-24-256-25: **Rockwell Automation ThinManager**

High level vulnerability: Externally Controlled Reference to a Resource in Another Sphere.

Rockwell Automation ThinManager | CISA

ICSA-24-254-01: **Viessmann Climate Solutions SE Vitogate 300**

Critical level vulnerabilities: Use of Hard-coded Credentials, Forced Browsing, Command Injection.

Viessmann Climate Solutions SE Vitogate 300 | CISA

ICSA-24-254-02: **iniNet Solutions SpiderControl SCADA Web Server**

High level vulnerability: Unrestricted Upload of File with Dangerous Type.

iniNet Solutions SpiderControl SCADA Web Server | CISA

ICSA-24-254-03: **Rockwell Automation SequenceManager**

High level vulnerability: Unquoted Search Path or Element.

Rockwell Automation SequenceManager | CISA

ICSMA-24-254-01: **BPL Medical Technologies PWS-01-BT and BPL Be Well Android Application**

Medium level vulnerability: Cleartext Transmission of Sensitive Information.

BPL Medical Technologies PWS-01-BT and BPL Be Well Android Application | CISA

ICSA-24-249-01: **Hughes Network Systems WL3000 Fusion Software**

High level vulnerabilities: Insufficiently Protected Credentials, Missing Encryption of Sensitive Data.

Hughes Network Systems WL3000 Fusion Software | CISA

ICSMA-24-249-01: **Baxter Connex Health Portal**

Critical level vulnerabilities: SQL Injection, Improper Access Control.

Baxter Connex Health Portal | CISA

ICSA-20-303-01: **Mitsubishi Electric MELSEC iQ-R, Q, and L Series (Update E)**

High level vulnerability: Uncontrolled Resource Consumption.

Mitsubishi Electric MELSEC iQ-R, Q and L Series (Update E) | CISA

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

High level vulnerability: Improper Resource Shutdown or Release.

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

ICSA-24-247-01: **LOYTEC Electronics LINX Series**

Critical level vulnerabilities: Cleartext Transmission of Sensitive Information, Missing Authentication for Critical Function, Cleartext Storage of Sensitive Information, Improper Access Control.

LOYTEC Electronics LINX Series | 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 September:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2021-20123 Draytek VigorConnect Path Traversal Vulnerability;
CVE-2021-20124 Draytek VigorConnect Path Traversal Vulnerability;
CVE-2024-7262 Kingsoft WPS Office Path Traversal Vulnerability;
CVE-2016-3714 ImageMagick Improper Input Validation Vulnerability;
CVE-2017-1000253 Linux Kernel PIE Stack Buffer Corruption Vulnerability;
CVE-2024-40766 SonicWall SonicOS Improper Access Control Vulnerability;
CVE-2024-38226 Microsoft Publisher Security Feature Bypass Vulnerability;
CVE-2024-43491 Microsoft Windows Update Remote Code Execution Vulnerability;
CVE-2024-38014 Microsoft Windows Installer Privilege Escalation Vulnerability;
CVE-2024-38217 Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability;
CVE-2024-8190 Ivanti Cloud Services Appliance OS Command Injection Vulnerability;
CVE-2024-43461 Microsoft Windows MSHTML Platform Spoofing Vulnerability;
CVE-2024-6670 Progress WhatsUp Gold SQL Injection Vulnerability;
CVE-2014-0497 Adobe Flash Player Integer Underflow Vulnerability;
CVE-2013-0643 Adobe Flash Player Incorrect Default Permissions Vulnerability;
CVE-2013-0648 Adobe Flash Player Code Execution Vulnerability;
CVE-2014-0502 Adobe Flash Player Double Free Vulnerability;
CVE-2024-27348 Apache HugeGraph-Server Improper Access Control Vulnerability;
CVE-2020-0618 Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability;
CVE-2019-1069 Microsoft Windows Task Scheduler Privilege Escalation Vulnerability;
CVE-2022-21445 Oracle JDeveloper Remote Code Execution Vulnerability;
CVE-2020-14644 Oracle WebLogic Server Remote Code Execution Vulnerability;
CVE-2024-7593 Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability;
CVE-2023-25280 D-Link DIR-820 Router OS Command Injection Vulnerability;
CVE-2020-15415 DrayTek Multiple Vigor Routers OS Command Injection Vulnerability;
CVE-2021-4043 Motion Spell GPAC Null Pointer Dereference Vulnerability;
CVE-2019-0344 SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability;
Links and more information:
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Five Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA

FBI, CISA, NSA, and US and International Partners Release Advisory on Russian Military Cyber Actors Targeting US and Global Critical Infrastructure

Federal Bureau of Investigation (FBI)—in partnership with CISA, the National Security Agency (NSA), and other U.S. and international partners—released a joint Cybersecurity Advisory Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure. This advisory provides overlapping cybersecurity industry cyber threat intelligence, tactics, techniques, and procedures (TTPs) and Indicators of Compromise (IOCs) associated with Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) cyber actors, both during and succeeding their deployment of the WhisperGate malware against Ukraine.

Links and more information:

FBI, CISA, NSA, and US and International Partners Release Advisory on Russian Military Cyber Actors Targeting US and Global Critical Infrastructure | CISA

Cisco Releases Security Updates for Cisco Smart Licensing Utility

Cisco released security updates to address two vulnerabilities (CVE-2024-20439 and CVE-2024-20440) in Cisco Smart Licensing Utility. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

Cisco Releases Security Updates for Cisco Smart Licensing Utility | CISA

Citrix Releases Security Updates for Citrix Workspace App for Windows

Citrix released security updates to address multiple vulnerabilities in the Citrix Workspace App for Windows. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Citrix Releases Security Updates for Citrix Workspace App for Windows | CISA

Ivanti Releases Security Updates for Endpoint Manager, Cloud Service Application, and Workspace Control

Ivanti released security updates to address multiple vulnerabilities in Ivanti Endpoint Manager, Cloud Service Application 4.6, and Workspace Control. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Ivanti Releases Security Updates for Endpoint Manager, Cloud Service Application, and Workspace Control | CISA

Microsoft Releases September 2024 Security Updates

Microsoft 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 September 2024 Security Updates | CISA

Adobe Releases Security Updates for Multiple Products
Adobe released security updates to address multiple 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 IOS XR Software
Cisco released security updates to address vulnerabilities in Cisco ISO XR 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 IOS XR Software | CISA

CISA Releases Analysis of FY23 Risk and Vulnerability Assessments
CISA has released an analysis and infographic detailing the findings from the 143 Risk and Vulnerability Assessments (RVAs) conducted across multiple critical infrastructure sectors in fiscal year 2023 (FY23).
Links and more information:
CISA Releases Analysis of FY23 Risk and Vulnerability Assessments | CISA

Ivanti Releases Security Update for Cloud Services Appliance
Ivanti has released a security update addressing an OS command injection vulnerability (CVE-2024-8190) affecting Ivanti Cloud Services Appliance (CSA) 4.6 (all versions before patch 519). A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Ivanti Releases Security Update for Cloud Services Appliance | CISA

New CISA Plan Aligns Federal Agencies in Cyber Defense
Cybersecurity and Infrastructure Security Agency (CISA) released the Federal Civilian Executive Branch (FCEB) Operational Cybersecurity Alignment (FOCAL) Plan. Developed in collaboration with FCEB agencies, this plan provides standard, essential components of enterprise operational cybersecurity and aligns the collective operational defense capabilities across the federal enterprise.
Links and more information:
New CISA Plan Aligns Federal Agencies in Cyber Defense | CISA

CISA and FBI Release Secure by Design Alert on Eliminating Cross-Site Scripting Vulnerabilities

CISA and FBI released a Secure by Design Alert, Eliminating Cross-Site Scripting Vulnerabilities, as a part of our ongoing effort to reduce the prevalence of vulnerability classes at scale. Vulnerabilities like cross-site scripting (XSS) continue to appear in software, enabling threat actors to exploit them. However, cross-site scripting vulnerabilities are preventable and should not be present in software products.
Links and more information:
CISA and FBI Release Secure by Design Alert on Eliminating Cross-Site Scripting Vulnerabilities | CISA

Apple Releases Security Updates for Multiple Products
Apple released security updates to address vulnerabilities in multiple Apple products. 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

VMware Releases Security Advisory for VMware Cloud Foundation and vCenter Server
VMware released a security advisory addressing vulnerabilities in the VMware Cloud Foundation and the vCenter Server. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.
Links and more information:
VMware Releases Security Advisory for VMware Cloud Foundation and vCenter Server | CISA

Ivanti Releases Admin Bypass Security Update for Cloud Services Appliance
Ivanti has released a security update to address an admin bypass vulnerability (CVE-2024-8963) affecting Ivanti Cloud Services Appliance (CSA) version 4.6. A cyber threat actor could exploit this vulnerability in conjunction with CVE-2024-8190–detailed in a Sept. 13 Ivanti security advisory–to take control of an affected system. This vulnerability impacts all versions prior to patch 519.
Links and more information:
Ivanti Releases Admin Bypass Security Update for Cloud Services Appliance | CISA

Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-45229
Versa Networks has released an advisory for a vulnerability (CVE-2024-45229) affecting Versa Director. A cyber threat actor could exploit this vulnerability to exercise unauthorized REST APIs.
Links and more information:
Versa Networks Releases Advisory for a Vulnerability in Versa Director, CVE-2024-45229 | CISA

Citrix Releases Security Updates for XenServer and Citrix Hypervisor
Citrix released security updates to address multiple vulnerabilities in XenServer and Citrix Hypervisor. A cyber threat actor could exploit some of these vulnerabilities to cause a denial of service condition.
Links and more information:
Citrix Releases Security Updates for XenServer and Citrix Hypervisor | CISA

Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means
CISA continues to respond to active exploitation of internet-accessible operational technology (OT) and industrial control systems (ICS) devices, including those in the Water and Wastewater Systems (WWS) Sector. Exposed and vulnerable OT/ICS systems may allow cyber threat actors to use default credentials, conduct brute force attacks, or use other unsophisticated methods to access these devices and cause harm.
Links and more information:
Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means | CISA

CISA Warns of Hurricane-Related Scams
As Hurricane Helene approaches, CISA urges users to remain on alert for potential malicious cyber activity. Fraudulent emails and social media messages—often containing malicious links or attachments—are common after major natural disasters. Exercise caution in handling emails with hurricane-related subject lines, attachments, or hyperlinks. In addition, be wary of social media pleas, texts, or door-to-door solicitations relating to severe weather events.
Links and more information:
CISA Warns of Hurricane-Related Scams | CISA

ASD's ACSC, CISA, and US and International Partners Release Guidance on Detecting and Mitigating Active Directory Compromises
Australian Signals Directorate Australian Cyber Security Centre (ASD ACSC), the Cybersecurity and Infrastructure Security Agency (CISA), and other U.S. and international partners released the joint guide Detecting and Mitigating Active Directory Compromises. This guide informs organizations of recommended strategies to mitigate common techniques used by malicious actors to compromise Active Directory.
Links and more information:
ASD's ACSC, CISA, and US and International Partners Release Guidance on Detecting and Mitigating Active Directory Compromises | CISA

Cisco Releases Security Updates for IOS and IOS XE Software
Cisco released its September 2024 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication to address vulnerabilities in IOS and IOS XE. 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 IOS and IOS XE Software | CISA

CISA's VDP Platform 2023 Annual Report Showcases Success

Cybersecurity and Infrastructure Security Agency (CISA) released its Vulnerability Disclosure Policy (VDP) Platform 2023 Annual Report, highlighting the service's remarkable success in 2023, its second full year of operation. Throughout 2023, CISA focused on advocating for the increased agency adoption of the VDP Platform, supporting federal civilian executive branch (FCEB) agencies in identifying vulnerabilities in their systems, and engaging the public security researcher community.

Links and more information:

CISA's VDP Platform 2023 Annual Report Showcases Success | CISA