2025 January, 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

Securing Industry 4.0: OT Cybersecurity Best Practices

The rapid integration of digital transformation and Industry 4.0 innovations has revolutionized industrial and critical infrastructure sectors, enhancing performance, agility, and efficiency. However, these advancements also increase interconnectivity between IT and OT systems, broadening the potential attack surface and exposing organizations to both insider and external cyber threats. Recent incidents highlight how vulnerabilities in these interconnected systems can lead to safety issues, financial losses, and reputational damage.

A significant example is a former contractor's alleged hacking attempt on a California water treatment facility, where stronger device-level security could have prevented unauthorized access. Unlike traditional intrusion detection systems (IDS) that monitor threats, zero-trust solutions provide proactive defense by securing devices and assets directly. This approach ensures authentication, access authorization, and traceability, enabling organizations to maintain operational integrity and continuity.

Zero-trust principles emphasize the need for layered security at the device and asset level, moving beyond reactive measures to a prevention-based strategy. By implementing robust access controls and authentication mechanisms, organizations can thwart unauthorized access, mitigate human errors, and block malicious activities before they impact operations.

Human error remains a critical vulnerability in cybersecurity. For instance, the 2021 incident at the Oldsmar water treatment facility in Florida demonstrated how simple mistakes, such as an employee pressing the wrong buttons, can jeopardize operations. A zero-trust solution could have prevented such errors by enforcing strict access controls and implementing device-level protections.

Adopting healthy cybersecurity hygiene, including regular training and secure practices, is essential to mitigating the risks posed by human errors. Industrial organizations must prioritize awareness and integrate asset-level safeguards to protect against all threats—whether accidental or deliberate.

Governments worldwide are responding to the escalating threats against critical infrastructure with stricter cybersecurity regulations. Singapore’s Cyber Security Agency introduced the Codes of Practice for Critical Infrastructure (CCoP 2.0), and the EU’s NIS2 directive enforces active cyber protection measures. Similarly, the U.S.

Environmental Protection Agency (EPA) has mandated public water systems to strengthen cybersecurity measures, including regular audits and inspections.

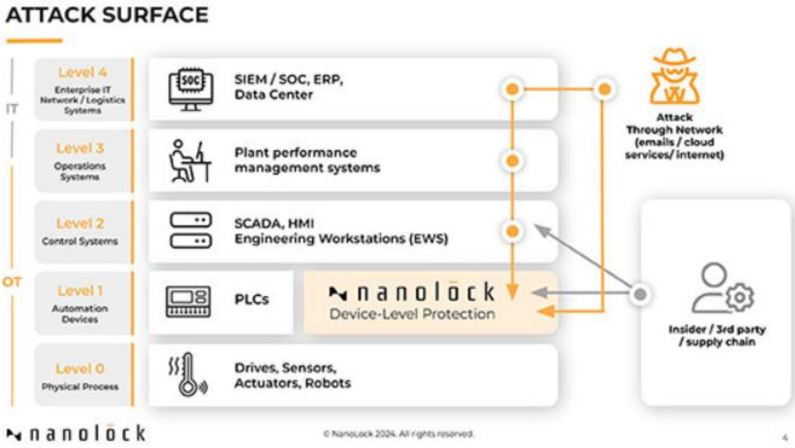
These regulations emphasize zero-trust philosophies, focusing on prevention through strict access control, activity logs, and authentication. Organizations failing to comply face severe penalties, such as fines of up to €10 million under NIS2. The trend underscores the importance of shifting from post-incident responses to proactive, prevention-based security measures.

Traditional cybersecurity approaches often focus solely on network protection, which addresses IT and OT connections but neglects the vulnerabilities of OT assets. Air-gapping networks - while helpful - does not sufficiently prevent unauthorized access or changes to critical OT assets, such as Programmable Logic Controllers (PLCs).

To achieve comprehensive security, organizations must adopt a layered approach. This includes maintaining network protections while integrating zero-trust principles at the device and asset level. By safeguarding critical OT assets, organizations can ensure operational integrity, prevent unauthorized modifications, and minimize the cascading effects of cyber incidents.

Conclusion

As Industry 4.0 advances, organizations must prioritize proactive cybersecurity measures to safeguard critical infrastructure. Zero-trust solutions at the device and asset level, combined with a layered security approach, are essential to mitigating risks, ensuring operational continuity, and complying with evolving regulations. By embracing these strategies, industrial organizations can fortify their defenses against an increasingly complex threat landscape.


ATTACK SURFACE
IT
OT
Level 4
Enterprise IT Network / Logistics Systems
Level 3
Operations Systems
Level 2
Control Systems
Level 1
Automation Devices
Level 0
Physical Process
SIEM / SOC, ERP, Data Center
Plant performance management systems
SCADA, HMI Engineering Workstations (EWS)
PLCs
nanolock
Device-Level Protection
Drives, Sensors, Actuators, Robots
Attack Through Network (emails / cloud services/ internet)
Insider / 3rd party / supply chain
nanolock
© NanoLock 2024. All rights reserved.
4

Source and more information available on the following link:

https://industrytoday.com/securing-industry-4-0-ot-cybersecurity-best-practices/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in February 2025:

- 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

- OT Railway Cybersecurity (OTCS)

https://informaconnect.com/ot-railway-cybersecurity-otcs/

- OT Security Expert (*Master OT/ICS security essentials for protecting critical infrastructure in the digital era*)

https://opswatacademy.com/courses/ot-security-expert

- CTR-008 - OT-Security Awareness E-Learning Course

https://www.yokogawa.com/eu/solutions/products-and-services/trainings-und-workshops/kompetenztrainings/ctr-008-ot-security-awareness-e-learning-course/

!NEW! in this feed:

- Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards

Comprehensive Guide to Industrial Cybersecurity with IEC 62443-3 Standards | EC-Council Learning

ICS conferences

In February 2025, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

S4x25

The ICS Village will also be setting up realistic ICS system in the Vulnerability Pavillion, where you can see our OT asset management, asset inventory, and vulnerability management capabilities live in action. The difference from last year will be that the system at the S4x25 Vulnerability Management Pavilion will be related to a specific physical process. Stop by the organizer booth for a demo, grab some swag, and connect with the organizer team about your OT environment.

Tampa, Florida USA; 10th – 13th February 2025

More details can be found on the following website:

https://www.industrialdefender.com/events/s4x25

Cyber Security For Critical Manufacturing Summit

Emerging cyber threats are increasingly disrupting our daily operations, as adversaries deploy advanced ransomware attacks on our critical systems and exploiting vulnerabilities within our manufacturing plants. To overcome these challenges, as well as those brought by an unstable geopolitical threat landscape and new innovations being introduced – strategies fit for tomorrow are required.

Join the top cyber security professionals from Europe's biggest manufacturers to network, learn, and be inspired. With 2 days of in-depth knowledge exchange, strategy planning and insight building through keynote presentations, real-life case studies, panel discussions, roundtables and networking breaks in Munich on 25th – 26th February 2025, ManuSec Europe is a must- attend for all senior IT & OT security leaders.

Munich, Germany; 25th – 26th February 2025

More details can be found on the following website:

https://europe.manusecevent.com/

ICS incidents

Ransomware Targeting Infrastructure Hits Telecom Namibia

The rising tide of ransomware attacks targeting critical infrastructure in Africa has taken a stark turn, with the recent breach of Telecom Namibia exemplifying the growing vulnerability of the region. The telecommunications giant suffered a ransomware attack by the Hunters International group, resulting in sensitive customer data being leaked on the dark web after the company refused to pay a ransom. This incident, alongside similar attacks on organizations such as South Africa's National Health Laboratory Service and Kenya's Urban Roads Authority, underscores the pressing need for robust cybersecurity measures across the continent.

The telecommunications, energy, and manufacturing sectors have emerged as key targets for cybercriminals in Africa, with ransomware accounting for one-third of all successful attacks in the region, according to Positive Technologies. Rapid digitization, geopolitical tensions, and inadequate cybersecurity measures are driving the surge in attacks. Alexey Lukatsky of Positive Technologies highlights how expanding digital networks and large data volumes make these sectors attractive to attackers seeking financial or geopolitical gains. Ransomware-as-a-service (RaaS) has intensified the threat landscape, allowing cybercriminals to focus on high-value targets like critical infrastructure providers. Avinash Singh from the University of Pretoria notes that African organizations are being used as testing grounds for new ransomware strategies. Beyond targeting primary entities, attackers are compromising third-party suppliers and distributing malicious software to amplify their reach.

With digital transformation outpacing cybersecurity implementation, the attack surface area across sectors such as telecommunications, energy, and manufacturing will continue to expand. Singh warns that Africa's geopolitical tensions further exacerbate these risks, especially as state-sponsored actors increasingly target the region.

African organizations must prioritize improving cybersecurity awareness among employees and customers while implementing secure practices and resilience strategies. Strengthening defenses against ransomware and fostering international collaboration will be crucial to counteract the escalating threats to critical infrastructure.

The source is available on the following link:

[Ransomware Targeting Infrastructure Hits Telecom Namibia]

Book recommendation

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

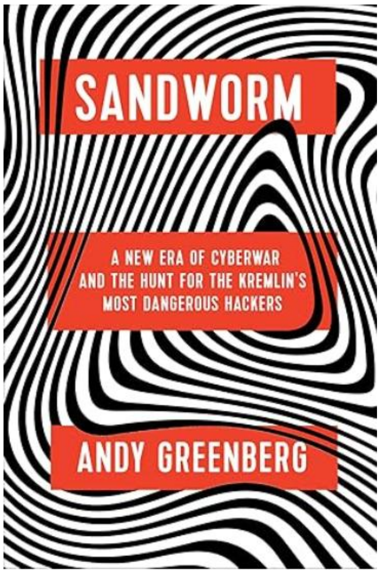
In 2014, the world witnessed the start of a mysterious series of cyberattacks. Targeting American utility companies, NATO, and electric grids in Eastern Europe, the strikes grew ever more brazen. They culminated in the summer of 2017, when the malware known as NotPetya was unleashed, penetrating, disrupting, and paralyzing some of the world's largest businesses—from drug manufacturers to software developers to shipping companies. At the attack's epicenter in Ukraine, ATMs froze. The railway and postal systems shut down. Hospitals went dark. NotPetya spread around the world, inflicting an unprecedented ten billion dollars in damage—the largest, most destructive cyberattack the world had ever seen. The hackers behind these attacks are quickly gaining a reputation as the most dangerous team of cyberwarriors in history: a group known as Sandworm. Working in the service of Russia's military intelligence agency, they represent a persistent, highly skilled force, one whose talents are matched by their willingness to launch broad, unrestrained attacks on the most critical infrastructure of their adversaries. They target government and private sector, military and civilians alike. A chilling, globe-spanning detective story, Sandworm considers the danger this force poses to our national security and stability. As the Kremlin's role in foreign government manipulation comes into greater focus, Sandworm exposes the realities not just of Russia's global digital offensive, but of an era where warfare ceases to be waged on the battlefield. It reveals how the lines between digital and physical conflict, between wartime and peacetime, have begun to blur—with world-shaking implications.

Author/Editor: Andy Greenberg (Author)

Year of issue: 2019

The book is available at the following link:

https://www.amazon.com/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers/dp/0385544405


SANDWORM
A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS
ANDY GREENBERG

ICS security news selection

Vulnerable Moxa devices expose industrial networks to attacks

Industrial networking and communications provider Moxa is warning of a high-severity and a critical vulnerability that impact various models of its cellular routers, secure routers, and network security appliances.

The two security issues allow remote attackers to get root privileges on vulnerable devices and to execute arbitrary commands, which could lead to arbitrary code execution. ...

Source and more information:

https://www.bleepingcomputer.com/news/security/vulnerable-moxa-devices-expose-industrial-networks-to-attacks/

Industrial cybersecurity coalitions rise to meet growing OT/ICS cyber threats, build awareness, take action

Across the globe, there is an increase in communities, associations, and alliances working toward information sharing and awareness engagement across the OT/ICS (operational technology/industrial control system) space in preparation for and mitigation against the increasing cyber threats and attacks. Industry coalitions are meant to promote active participation in interaction among peers to allow for the exchange of information, competencies, and skills among cybersecurity professionals.

Set up by the International Society of Automation (ISA), the ISA Global Cybersecurity Alliance (ISAGCA) is a collaborative platform to enhance awareness, education, preparedness, standardization, and knowledge sharing in OT cybersecurity. Comprising over 50 member companies with a collective revenue exceeding US$1.5 trillion and more than 2,400 global locations, ISAGCA was formed to tackle cybersecurity threats and vulnerabilities that pose significant risks to facilities, processes, and community safety. ...

Source and more information:

https://industrialcyber.co/features/industrial-cybersecurity-coalitions-rise-to-meet-growing-ot-ics-cyber-threats-build-awareness-take-action/

Western Security Agencies Share Advice on Selecting OT Products

CISA and several other Western security agencies have published guidance to help operational technology (OT) owners and operators select secure products.

The authoring agencies warn that threat actors are targeting particular OT products rather than specific organizations, pointing out that vulnerable OT products can grant attackers access to the systems of multiple victims across various critical infrastructure sectors. …

Source and more information:

https://www.securityweek.com/western-security-agencies-share-advice-on-selecting-ot-products/

War Game Pits China Against Taiwan in All-Out Cyberwar

At Black Hat and DEF CON, cybersecurity experts were asked to game out how Taiwan could protect its communications and power infrastructure in case of invasion by China.

If China attacked Taiwan, how could Taiwan defend its critical communications infrastructure from cyberattack?

Last year, Dr. Nina A. Kollars and Jason Vogt — both associate professors at the US Naval War College (USNWC) Cyber and Innovation Policy Institute (CIPI) — designed a war game to inspire some novel strategies. They enlisted government and private sector cybersecurity experts at Black Hat and DEF CON to participate, and presented the results at ShmooCon earlier this month. …

Source and more information:

https://www.darkreading.com/threat-intelligence/war-game-pits-china-against-taiwan-cyberwar

Building Automation Protocols Increasingly Targeted in OT Attacks: Report

Industrial automation protocols continue to be the most targeted in OT attacks, but building automation systems have been increasingly targeted.

Industrial automation protocols continue to be the most targeted in attacks aimed at operational technology (OT), but building automation systems have been increasingly targeted, according to a new report from cybersecurity firm Forescout.

Forescout on Monday published its 2024 Threat Roundup report, which is based on attacks recorded by the company's honeypots last year, including port scanning, brute force attacks, and attempts to exploit vulnerabilities. …

Source and more information:

https://www.securityweek.com/building-automation-protocols-increasingly-targeted-in-ot-attacks-report/

David Gee appointed as ambassador for CI-ISAC Australia to bolster critical infrastructure cybersecurity

CI-ISAC Australia, a not-for-profit organization focused on cybersecurity and operating on a membership model, has appointed David Gee as a new ambassador for the Critical Infrastructure – Information Sharing and Analysis Centre (CI-ISAC) in Australia, effective Jan. 30, 2025. Gee brings extensive experience to this role. With over 25 years of leadership in technology, cybersecurity, and risk management, he has played a key role in transforming IT infrastructures and enhancing digital security for major organizations worldwide. …

Source and more information:

https://industrialcyber.co/news/david-gee-appointed-as-ambassador-for-ci-isac-australia-to-bolster-critical-infrastructure-cybersecurity/

How Interlock Ransomware Infects Healthcare Organizations

Ransomware attacks have reached an unprecedented scale in the healthcare sector, exposing vulnerabilities that put millions at risk. Recently, UnitedHealth revealed that 190 million Americans had their personal and healthcare data stolen during the Change Healthcare ransomware attack, a figure that nearly doubles the previously disclosed total. This breach shows just how deeply ransomware can infiltrate critical systems, leaving patient trust and care hanging in the balance.

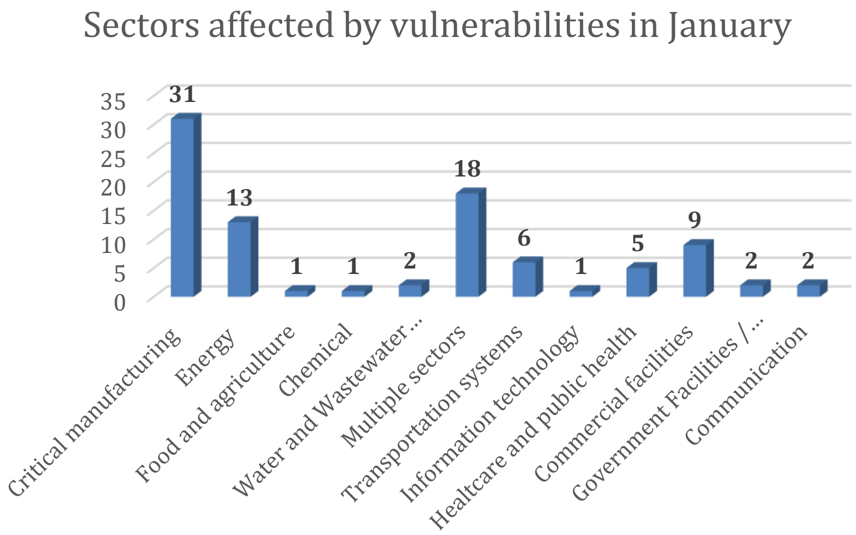
One of the groups that targets this already fragile sector is the Interlock ransomware group. Known for their calculated and sophisticated attacks, they focus on hospitals, clinics, and other medical service providers.

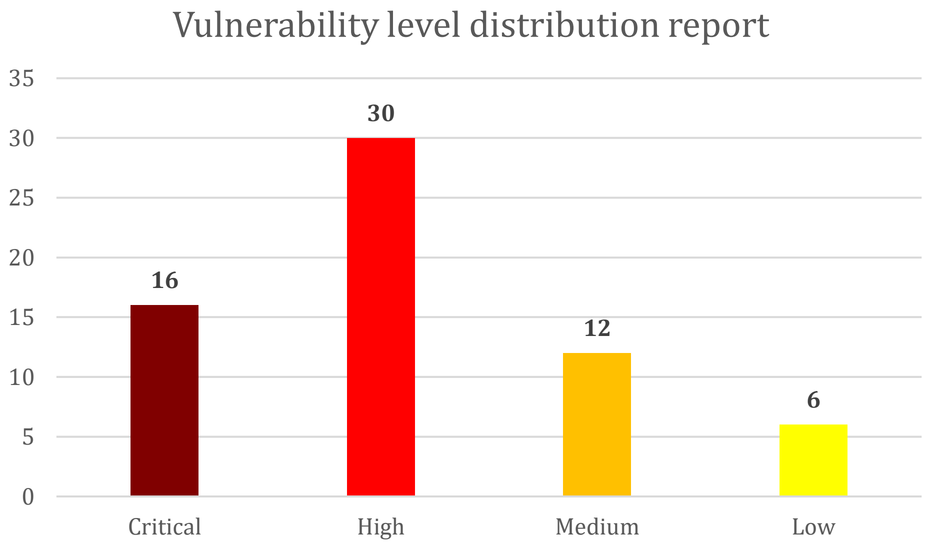
Source and more information:

https://thehackernews.com/2025/01/how-interlock-ransomware-infects.html

ICS vulnerabilities

In January 2025, 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:





ICSA-25-030-01: **Hitachi Energy UNEM**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Argument Injection, Heap-based Buffer Overflow, Improper Certificate Validation, Use of Hard-coded Password, Improper Restriction of Excessive Authentication Attempts, Cleartext Storage of Sensitive Information, Incorrect User Management.

Hitachi Energy UNEM | CISA

ICSA-25-030-02: **New Rock Technologies Cloud Connected Devices**

Critical level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Neutralization of Wildcards or Matching Symbols.

New Rock Technologies Cloud Connected Devices | CISA

ICSA-25-030-03: **Schneider Electric System Monitor Application in Harmony and Pro-face PS5000 Legacy Industrial PCs**

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

Schneider Electric System Monitor Application in Harmony and Pro-face PS5000 Legacy Industrial PCs | CISA

ICSA-25-030-04: **Rockwell Automation KEPServer**

High level vulnerability: Uncontrolled Resource Consumption.

Rockwell Automation KEPServer | CISA

ICSA-25-030-05: **Rockwell Automation FactoryTalk AssetCentre**

Critical level vulnerabilities: Inadequate Encryption Strength, Insufficiently Protected Credentials.

Rockwell Automation FactoryTalk AssetCentre | CISA

ICSMA-25-030-01: **Contec Health CMS8000 Patient Monitor**

Critical level vulnerabilities: Out-of-bounds Write, Hidden Functionality (Backdoor), Privacy Leakage.

Contec Health CMS8000 Patient Monitor | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update B)**

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

Mitsubishi Electric Multiple FA Engineering Software Products (Update B) | CISA

ICSMA-22-244-01: **Contec Health CMS8000 Patient Monitor (Update A)**

High level vulnerabilities: Improper Physical Access Control, Allocation of Resources Without Limits or Throttling, Use of Hard-Coded Credentials, Active Debug Code, Unprotected Primary Channel.

Contec Health CMS8000 Patient Monitor (Update A) | CISA

ICSA-25-028-01: **B&R Automation Runtime**

High level vulnerability: Use of a Broken or Risky Cryptographic Algorithm.

B&R Automation Runtime | CISA

ICSA-25-028-02: **Schneider Electric Power Logic**

High level vulnerabilities: Authorization Bypass Through User-Controlled Key, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Schneider Electric Power Logic | CISA

ICSA-25-028-03: **Rockwell Automation FactoryTalk**

Critical level vulnerabilities: Incorrect Authorization, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection').

Rockwell Automation FactoryTalk | CISA

ICSA-25-028-04: **Rockwell Automation FactoryTalk**

High level vulnerabilities: Incorrect Permission Assignment for Critical Resource, Improper Control of Generation of Code ('Code Injection').

Rockwell Automation FactoryTalk | CISA

ICSA-25-028-05: **Rockwell Automation DataMosaix Private Cloud**

Critical level vulnerabilities: Exposure of Sensitive Information to an Unauthorized Actor, Dependency on Vulnerable Third-Party Component.

Rockwell Automation DataMosaix Private Cloud | CISA

ICSA-25-028-06: **Schneider Electric RemoteConnect and SCADAPack x70 Utilities**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric RemoteConnect and SCADAPack x70 Utilities | CISA

ICSMA-24-352-01: **BD Diagnostic Solutions Products (Update A)**

High level vulnerability: Use of Default Credentials.

BD Diagnostic Solutions Products (Update A) | CISA

ICSA-25-023-01: **mySCADA myPRO Manager**

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

mySCADA myPRO Manager | CISA

ICSA-25-023-02: **Hitachi Energy RTU500 Series Product**

High level vulnerability: Improperly Implemented Security Check for Standard.

Hitachi Energy RTU500 Series Product | CISA

ICSA-25-023-03: **Schneider Electric EVlink Home Smart and Schneider Charge**

High level vulnerability: Cleartext Storage of Sensitive Information.

Schneider Electric EVlink Home Smart and Schneider Charge | CISA

ICSA-25-023-04: **Schneider Electric Easergy Studio**

High level vulnerability: Improper Privilege Management.

Schneider Electric Easergy Studio | CISA

ICSA-25-023-05: **Schneider Electric EcoStruxure Power Build Rapsody**

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

Schneider Electric EcoStruxure Power Build Rapsody | CISA

ICSA-25-023-06: **HMS Networks Ewon Flexy 202**

Medium level vulnerability: Cleartext Transmission of Sensitive Information.

HMS Networks Ewon Flexy 202 | CISA

ICSA-25-021-01: **Traffic Alert and Collision Avoidance System (TCAS) II**

High level vulnerabilities: Reliance on Untrusted Inputs in a Security Decision, External Control of System or Configuration Setting.

Traffic Alert and Collision Avoidance System (TCAS) II | CISA

ICSA-25-021-02: **Siemens SIMATIC S7-1200 CPUs**

High level vulnerability: Cross-Site Request Forgery.

Siemens SIMATIC S7-1200 CPUs | CISA

ICSA-25-021-03: **ZF Roll Stability Support Plus (RSSPlus)**

Medium level vulnerability: Authentication Bypass By Primary Weakness.

ZF Roll Stability Support Plus (RSSPlus) | CISA

ICSA-25-016-01: **Siemens Mendix LDAP**

High level vulnerability: LDAP Injection.

Siemens Mendix LDAP | CISA

ICSA-25-016-02: **Siemens Industrial Edge Management**

Low level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Siemens Industrial Edge Management | CISA

ICSA-25-016-03: **Siemens Siveillance Video Camera**

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

Siemens Siveillance Video Camera | CISA

ICSA-25-016-04: **Siemens SIPROTEC 5 Products**

High level vulnerability: Files or Directories Accessible to External Parties.

Siemens SIPROTEC 5 Products | CISA

ICSA-25-016-05: **Fuji Electric Alpha5 SMART**

High level vulnerability: Stack-based Buffer Overflow.

Fuji Electric Alpha5 SMART | CISA

ICSA-25-016-06: **Hitachi Energy FOX61x, FOXCST, and FOXMAN-UN Products**

Low level vulnerability: Improper Validation of Certificate with Host Mismatch.

Hitachi Energy FOX61x, FOXCST, and FOXMAN-UN Products | CISA

ICSA-25-016-07: **Hitachi Energy FOX61x Products**

Low level vulnerability: Relative Path Traversal.

Hitachi Energy FOX61x Products | CISA

ICSA-25-016-08: **Schneider Electric Data Center Expert**

High level vulnerabilities: Improper Verification of Cryptographic Signature, Missing Authentication for Critical Function.

Schneider Electric Data Center Expert | CISA

ICSA-24-058-01: **Mitsubishi Electric Multiple Factory Automation Products (Update A)**

Medium level vulnerability: Insufficient Resource Pool.

Mitsubishi Electric Multiple Factory Automation Products (Update A) | CISA

ICSA-25-010-03: **Delta Electronics DRASimuCAD (Update A)**

High level vulnerabilities: Out-of-bounds Write, Type Confusion.

Delta Electronics DRASimuCAD (Update A) | CISA

ICSA-24-191-05: **Johnson Controls Inc. Software House C•CURE 9000 (Update A)**

High level vulnerability: Incorrect Default Permissions.

Johnson Controls Software House C•CURE 9000 (Update A) | CISA

ICSA-24-030-02: **Mitsubishi Electric FA Engineering Software Products (Update B)**

Critical level vulnerabilities: Missing Authentication for Critical Function, Unsafe Reflection.

Mitsubishi Electric FA Engineering Software Products (Update B) | CISA

SSA-404759: **Siveillance Video Camera Drivers (Update: 1.1.)**

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

SSA-404759

SSA-999588: **Siemens User Management Component (UMC) Before V2.11.2 (Update: 1.7.)**

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

SSA-876787: **Siemens SIMATIC S7-1500 and S7-1200 CPUs (Update: 1.3.)**

Medium level vulnerability: URL Redirection to Untrusted Site ('Open Redirect').

SSA-876787

SSA-871035: **Siemens Engineering Platforms Before V19 (Update: 1.1.)**

High level vulnerability: Deserialization of Untrusted Data.

SSA-871035

SSA-773256: **Siemens Industrial Products (Update: 1.3.)**

High level vulnerability: Improper Input Validation.

SSA-773256

SSA-730482: **Siemens SIMATIC WinCC (Update: 1.2.)**

Medium level vulnerability: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').

SSA-730482

SSA-723487: **Siemens SCALANCE, RUGGEDCOM and Related Products (Update: 1.4.)** **Critical** level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-711309: **Siemens SIMATIC Products (Update: 2.3.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309

SSA-690517: **Siemens SCALANCE W-700 IEEE 802.11ax Family (Update: 1.2.)**

High level vulnerabilities: 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

SSA-629254: **Siemens SIMATIC SCADA and PCS 7 systems (Update: 1.3.)**

Critical level vulnerability: Execution with Unnecessary Privileges.

SSA-629254

SSA-593272: **IP-Stack based Industrial Devices (Update: 2.3.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-593272

SSA-482757: **Siemens S7-1500 CPU devices (Update: 1.5.)**

Low level vulnerability: Missing Immutable Root of Trust in Hardware.

SSA-482757

SSA-446448: **Siemens PROFINET Stack Integrated on Interniche Stack (Update: 2.3.)** **Medium** level vulnerability: Uncontrolled Resource Consumption.

SSA-446448

SSA-413565: **Siemens SCALANCE Products (Update: 1.4.)**

High level vulnerabilities: Improper Control of Generation of Code ('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.

SSA-413565

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update: 2.2.)** **Critical** level vulnerabilities: Multiple.

SSA-398330

SSA-097435: **Siemens Mendix Runtime (Update: 1.8.)**

Medium level vulnerability: Observable Response Discrepancy.

SSA-097435

SSA-054046: **Web Server of Siemens SIMATIC S7-1500 CPUs (Update: 1.2.)**

Medium level vulnerability: Authentication Bypass Using an Alternate Path or Channel.

SSA-054046

SSA-039007: **Siemens User Management Component (UMC) (Update: 1.3.)**

Critical level vulnerability: Heap-based Buffer Overflow.

SSA-039007

ICSA-25-014-01: **Hitachi Energy FOXMAN-UN**

Critical level vulnerabilities: Authentication Bypass Using an Alternate Path or Channel, Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), Heap-based Buffer Overflow, Incorrect User Management, Improper Certificate Validation, Improper Restriction of Excessive Authentication Attempts, Use of Hard-coded Password, Cleartext Storage of Sensitive Information.

Hitachi Energy FOXMAN-UN | CISA

ICSA-25-014-02: **Schneider Electric Vijeo Designer**

High level vulnerability: Improper Privilege Management.

Schneider Electric Vijeo Designer | CISA

ICSA-25-014-03: **Schneider Electric EcoStruxure**

Medium level vulnerability: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Schneider Electric EcoStruxure | CISA

ICSA-25-014-04: **Belledonne Communications Linphone-Desktop**

High level vulnerability: NULL Pointer Dereference.

Belledonne Communications Linphone-Desktop | CISA

ICSA-25-010-01: **Schneider Electric PowerChute Serial Shutdown**

Medium level vulnerability: Improper Authentication.

Schneider Electric PowerChute Serial Shutdown | CISA

ICSA-25-010-02: **Schneider Electric Harmony HMI and Pro-face HMI Products**

High level vulnerability: Use of Unmaintained Third-Party Components.

Schneider Electric Harmony HMI and Pro-face HMI Products | CISA

ICSA-25-010-03: **Delta Electronics DRASimuCAD**

High level vulnerabilities: Out-of-bounds Write, Type Confusion.

Delta Electronics DRASimuCAD | CISA

ICSA-24-345-06: **Rockwell Automation Arena (Update A)**

High level vulnerabilities: Use After Free, Out-of-bounds Write, Improper Initialization, Out-of-bounds Read, Dependency on Vulnerable Third-Party Component.

Rockwell Automation Arena (Update A) | CISA

ICSA-25-007-01: **ABB ASPECT-Enterprise, NEXUS, and MATRIX Series Products**

Critical level vulnerabilities: Files or Directories Accessible to External Parties, Improper Validation of Specified Type of Input, Cleartext Transmission of Sensitive Information, Cross-site Scripting, Server-Side Request Forgery (SSRF), Improper Neutralization of Special Elements in Data Query Logic, Allocation of Resources Without Limits or Throttling, Weak Password Requirements, Cross-Site Request Forgery (CSRF), Use of Weak Hash, Code Injection, PHP Remote File Inclusion, External Control of System or Configuration Setting, Insufficiently Protected Credentials, Unrestricted Upload of File with Dangerous Type, Absolute Path Traversal, Use of Default Credentials, Off-by-one Error, Use of Default Password, Session Fixation.

ABB ASPECT-Enterprise, NEXUS, and MATRIX Series Products | CISA

ICSA-25-007-02: **Nedap Librix Ecoreader**

Critical level vulnerability: Missing Authentication for Critical Function.

Nedap Librix Ecoreader | 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 2025 January:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2024-41713 Mitel MiCollab Path Traversal Vulnerability;
CVE-2024-55550 Mitel MiCollab Path Traversal Vulnerability;
CVE-2020-2883 Oracle WebLogic Server Unspecified Vulnerability;
CVE-2025-0282 Ivanti Connect Secure Vulnerability;
CVE-2024-55591 Fortinet FortiOS Authorization Bypass Vulnerability;
CVE-2025-21333 Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability;
CVE-2025-21334 Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability;
CVE-2025-21335 Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability;
CVE-2024-50603 Aviatrix Controllers OS Command Injection Vulnerability;
CVE-2020-11023 JQuery Cross-Site Scripting (XSS) Vulnerability;
CVE-2025-23006 SonicWall SMA1000 Appliances Deserialization Vulnerability;
CVE-2025-24085 Apple Multiple Products Use-After-Free Vulnerability;
Links and more information:
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Vulnerability to the KEV Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

Ivanti Releases Security Updates for Connect Secure, Policy Secure, and ZTA Gateways
Ivanti released security updates to address vulnerabilities (CVE-2025-0282, CVE-2025-0283) in Ivanti Connect Secure, Policy Secure, and ZTA Gateways. A cyber threat actor could exploit CVE-2025-0282 to take control of an affected system.
Links and more information:
Ivanti Releases Security Updates for Connect Secure, Policy Secure, and ZTA Gateways | CISA

CISA Releases the Cybersecurity Performance Goals Adoption Report
CISA released the Cybersecurity Performance Goals Adoption Report to highlight how adoption of Cybersecurity Performance Goals (CPGs) benefits our nation's critical infrastructure sectors. Originally released in October 2022, CISA's CPGs are voluntary

practices that critical infrastructure owners can take to protect themselves against cyber threats.

Links and more information:

CISA Releases the Cybersecurity Performance Goals Adoption Report | CISA

CISA and US and International Partners Publish Guidance on Priority Considerations in Product Selection for OT Owners and Operators

CISA—along with U.S. and international partners—released joint guidance Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products. As part of CISA's Secure by Demand series, this guidance focuses on helping customers identify manufacturers dedicated to continuous improvement and achieving a better cost balance, as well as how Operational Technology (OT) owners and operators should integrate secure by design elements into their procurement process.

Links and more information:

CISA and US and International Partners Publish Guidance on Priority Considerations in Product Selection for OT Owners and Operators | CISA

CISA Releases the JCDC AI Cybersecurity Collaboration Playbook and Fact Sheet

CISA released the JCDC AI Cybersecurity Collaboration Playbook and Fact Sheet to foster operational collaboration among government, industry, and international partners and strengthen artificial intelligence (AI) cybersecurity. The playbook provides voluntary information-sharing processes that, if adopted, can help protect organizations from emerging AI threats.

Links and more information:

CISA Releases the JCDC AI Cybersecurity Collaboration Playbook and Fact Sheet | CISA

Fortinet Releases Security Updates for Multiple Products

Fortinet released security updates to address vulnerabilities in multiple Fortinet products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Fortinet Releases Security Updates for Multiple Products | CISA

Ivanti Releases Security Updates for Multiple Products

Ivanti released security updates to address vulnerabilities in Ivanti Avalanche, Ivanti Application Control Engine, and Ivanti EPM.

Links and more information:

Ivanti Releases Security Updates for Multiple Products | CISA

Microsoft Releases January 2025 Security Updates
Microsoft released security updates to address vulnerabilities in multiple Microsoft products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.
Links and more information:
Microsoft Releases January 2025 Security Updates | CISA

Adobe Releases Security Updates for Multiple Products
Adobe released security updates to address vulnerabilities in multiple Adobe software products including Adobe Photoshop, Animate, and Illustrator for iPad. 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

CISA Releases Microsoft Expanded Cloud Logs Implementation Playbook
CISA released the Microsoft Expanded Cloud Logs Implementation Playbook to help organizations get the most out of Microsoft's newly introduced logs in Microsoft Purview Audit (Standard). This step-by-step guide enables technical personnel to better detect and defend against advanced intrusion techniques by operationalizing expanded cloud logs.
Links and more information:
CISA Releases Microsoft Expanded Cloud Logs Implementation Playbook | CISA

CISA and Partners Release Call to Action to Close the National Software Understanding Gap
CISA—in partnership with the Defense Advanced Research Projects Agency (DARPA), the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E), and the National Security Agency (NSA)—published Closing the Software Understanding Gap. This report urgently implores the U.S. government to take decisive and coordinated action.
Links and more information:
CISA and Partners Release Call to Action to Close the National Software Understanding Gap | CISA

Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications
The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory in response to exploitation in September 2024 of vulnerabilities in Ivanti Cloud Service Appliances (CSA): CVE-2024-8963, an administrative bypass vulnerability; CVE-2024-9379, a SQL injection vulnerability; and CVE-2024-8190 and CVE-2024-9380, remote code execution vulnerabilities.
Links and more information:
Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications | CISA

CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware

CISA released a fact sheet, Contec CMS8000 Contains a Backdoor, detailing an analysis of three firmware package versions of the Contec CMS8000, a patient monitor used by the U.S. Healthcare and Public Health (HPH) sector. Analysts discovered that an embedded backdoor function with a hard-coded IP address, CWE – 912: Hidden Functionality (CVE-2025-0626), and functionality that enables patient data spillage, CWE – 359: Exposure of Private Personal Information to an Unauthorized Actor (CVE-2025-0683), exists in all versions analyzed.

Links and more information:

CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware | CISA