BLACK CELL
Protecting critical infrastructures

Critical Systems security feed

2026 June

2026 June, Critical Systems security feed

Black Cell is committed for the security of Critical Systems and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS, OT and critical infrastructure operators and provides information on vulnerabilities, podcasts, trainings, conferences, books, and incidents on the subject of ICS and OT security. Black Cell provides recommendations and solutions to establish a resilient and robust critical systems security organization. If you're interested in critical systems security, feel free to contact our experts at info@blackcell.io.

List of Contents

1. Critical systems security practices, recommendations

10 Best Practices for Operational Technology (OT) Security

As the integration of digital technologies in industrial processes continues to advance, the need for robust cybersecurity measures in Operational Technology (OT) environments becomes paramount. OT systems control and monitor physical devices and processes and are vital to businesses, regardless of whether they are part of manufacturing facilities, CNC machines, or critical infrastructure like airports, banks, and utilities.

The standard cybersecurity advice for IT and security managers of companies with OT networks is to make efforts to separate them from the regular networks. That being said, CISOs often talk about the separation of networks and the basic fundamentals that go with it, but they don't make sure that these fundamentals are implemented well or consider the possible ramifications.

Recently, for example, we spoke to a client that asked for advice about different cybersecurity matters. Although the client had acceptable security, they were completely unaware that the OT network was connected by the IT staff to one of the administrative networks and basic security practices were not in place, thus potentially opening it to the outside world.

Here are ten best practices for securing operational technology (OT) cyber environments.

1. Risk Assessment and Asset Inventory
2. Access Control and Authentication
3. Network Segmentation
4. Patch Management and Vulnerability Assessment
5. Remote assistance and maintenance
6. Intrusion Detection and Prevention Systems (IDPS)
7. Security Information and Event Management (SIEM)
8. Employee Training and Awareness
9. Incident Response and Business Continuity Planning
10. Regulatory Compliance and Standards

More information about the best practices can be found at the link below.

Source and more information:

[10 Best Practices for Operational Technology (OT) Security — CYE]

2. Critical systems security conferences

In July 2026, the following ICS/SCADA/OT security conferences and workshops will be organized (not comprehensive):

The 16th IEEE International Conference on CYBER Technology in Automation, Control, and Intelligent Systems

The scope of IEEE CYBER 2026 focuses on the intersection of Cyber-Physical Systems (CPS) and Industrial Intelligence, specifically targeting the integration of advanced robotics, automation, and intelligent sensing. Key areas include the development of autonomous systems, human-robot collaboration, and brain-machine interfaces, alongside emerging applications in carbon neutrality and digital twin environments. By bridging foundational control theory with real-world industrial and healthcare automation, the conference provides a comprehensive platform for advancing the "Physical-Cyber-Human" triad in modern engineering.

Florence, Italy; 21st – 25th July 2026

More details can be found on the following website:

Home - IEEE-CYBER 2026

OT SCADA CON 2026

Join for a unique community conference event all about Industrial Automation technology in Houston, TX!

Dive into the world of operational technology (OT) and supervisory control and data acquisition (SCADA) and related disciplines with industry experts and fellow enthusiasts.

Connect, learn, and network in person at this one-of-a-kind conference for the industrial automation community.

Houston, Texas, USA; 22nd – 24th July 2026

More details can be found on the following website:

OT SCADA CON 2026 | July 22, 2026 - July 24, 2026

24th IEEE International Conference on Industrial Informatics

This conference provides a forum for presentation and discussion of the state-of-art and future perspectives of industrial information technologies. Industry experts, researchers and academics are gathering together to share ideas and experiences surrounding frontier technologies, breakthroughs, innovative solutions, research results, as well as initiatives related to industrial informatics and their applications.

This is the 24th edition of the conference, with most recent previous editions being hosted as follows: Helsinki-Espoo, Finland (2019); Coventry, UK (2020); Palma de Mallorca/Online, Spain

(2021); Perth, Australia (2022); Lemgo, Germany (2023); Beijing, China (2024); and Kunming, China (2025).

Melbourne, Australia; 26th – 29th July 2026

More details can be found on the following website:

IEEE INDIN 2026 | 26-29 July 2026 | Melbourne, Australia :: IEEE International Conference on Industrial Informatics

3. Critical systems security incidents

Pharma giant West Pharmaceutical discloses ransomware attack disrupting operations

On May 4, 2026, West Pharmaceutical Services - a critical multi-national manufacturer generating over $3 billion in net sales - detected a severe network intrusion that was later confirmed to be a material ransomware attack. The incident involved both the exfiltration of corporate data and the encryption of vital information technology (IT) systems. In response to the breach, West Pharmaceutical Services was forced to immediately execute containment protocols, which included taking significant portions of its network offline, severing access to enterprise systems, and isolating its on-premise infrastructure. While these defensive measures were necessary to halt the threat actor's lateral movement, they triggered immediate and widespread disruptions to the company's manufacturing operations, shipping schedules, and shared service functions across its global footprint. The operational fallout of this network isolation highlights the severe vulnerability of modern, interconnected Industrial Control Systems (ICS) and Manufacturing Execution Systems (MES). West Pharmaceutical Services operates 50 certified manufacturing, distribution, and research and development facilities worldwide, producing over 41 billion components and devices annually - including vial containment systems and prefillable syringes essential for life-saving medical treatments. The abrupt shutdown of enterprise networks effectively paralyzed the digitized workflows that govern these automated production lines. Without access to centralized IT databases, critical processes such as computerized raw material receiving, automated quality assurance, inventory tracking, and synchronized shipping functions were completely halted, causing physical backlogs and production freezes across facilities in the Americas, Europe, and the Asia-Pacific region.

Resiliency and remediation efforts began immediately, with West enlisting third-party cybersecurity experts from Palo Alto Networks Unit 42 to lead the incident response. By May 13, nearly a week after the initial detection, Unit 42 confirmed that the unauthorized activity had been successfully contained and the immediate risk to the operational environment mitigated. The recovery strategy relies heavily on a comprehensive rebuild of the impacted IT infrastructure. Teams are systematically restoring systems using clean backups that predate the known window of compromise to prevent threat actor re-entry, while keeping unverified segments entirely isolated from the production network. From an information security governance perspective, this incident serves as a stark reminder of the downstream supply chain risks inherent to the pharmaceutical and biotechnology sectors. Although West has managed to restore its core enterprise systems and restart critical shipping and manufacturing processes at select sites, a definitive timeline for full capacity recovery remains undetermined. The disruption underscores the critical need for industrial organizations to establish robust IT/OT segmentation. Maintaining the capability to isolate compromised corporate networks while sustaining standalone, localized manufacturing floor operations is paramount to mitigating systemic risk and ensuring business continuity during a targeted ransomware event.

The source is available at the following link:

[West Pharma ransomware attack disrupts operations | Cybernews]

Iranian Cyber Group Handala Claims Cal Water Hack

In a recent cyber campaign, the Iran-linked threat actor tracked as Handala (also known as Storm-0842 or Void Manticore) claimed to have breached California Water Service (Cal Water), one of the largest investor-owned water utilities in the United States, servicing approximately two million customers. The threat actor subsequently published 5 gigabytes of exfiltrated data, which included database exports of personally identifiable information (PII) such as customer billing records, payment histories, and account numbers. While the theft of corporate and customer data poses severe compliance and reputational challenges, the technical parameters of the breach reveal a far more alarming narrative: the successful compromise and enumeration of applications deeply intertwined with the utility's Operational Technology (OT) and critical infrastructure perimeter.

According to threat intelligence assessments, the initial access vector or pivotal entry point was not a traditional corporate IT system, but rather an active instance of Cal Water's RTKBase platform. RTKBase is an open-source Global Navigation Satellite System (GNSS) base station manager used to stream high-precision GPS correction data across multiple utility districts via the NTRIP (Networked Transport of RTCM via Internet Protocol) network. At the time of the compromise, the targeted instance had been running continuously for nearly 783 hours, streaming live operational telemetry across seven distinct district mountpoints. By successfully infiltrating this specialized network, Handala was able to exfiltrate administrative credentials for the RTKBase platform itself, cleartext NTRIP source passwords, and comprehensive IP address enumerations of the utility's district-level NTRIP infrastructure. The threat actor then leveraged this exposed interface to move laterally into the business environment, ultimately reaching the distinct customer billing database.

The strategic significance of targeting a GNSS/NTRIP base station architecture underscores a growing trend where adversaries exploit niche, internet-exposed industrial applications to bridge the gap between IT and OT environments. In modern utility automation, high-precision geospatial and timing data streamed by platforms like RTKBase are frequently utilized by field assets, supervisory systems, and telemetry units. Although a direct disruption to Industrial Control Systems (ICS) or water treatment physical processes has not been confirmed in this specific incident - and the hackers claimed they voluntarily chose not to disrupt water access - the technical exposure of administrative passwords and network topologies at the district level implies that the adversary achieved the requisite visibility to do so.

Furthermore, Handala's historical operational profile elevates this incident from a standard data breach to a critical national infrastructure threat precursor. Attributed by the US government to Iran's Ministry of Intelligence and Security (MOIS), Handala possesses a documented toolkit consisting of destructive custom wipers (such as Handala Wiper and Hamsa Wiper) and Master Boot Record (MBR)-overwriting capabilities. The group is notorious for a multi-stage execution pattern where an initial data exfiltration or psychological operation serves as a precursor to subsequent destructive attacks within the same campaign cycle. Consequently, the leak of critical NTRIP routing data and master credentials indicates that the threat actor has effectively mapped Cal Water's peripheral industrial network. Immediate remediation requirements dictate that the utility treat this breach as an active threat, rotate all

exposed administrative credentials, isolate the RTKBase network through strict IT/OT segmentation, and audit access logs to prevent a destructive follow-on cyberattack.

The source is available at the following link:

Iranian Cyber Group Handala Claims Cal Water Hack - SecurityWeek

Cyberattack disrupts Mackay Sugar operations, exposing growing agri-industrial cyber risks

A significant cyberattack has severely disrupted operations at Mackay Sugar, Australia's second-largest raw sugar producer, forcing an immediate operational shutdown at its Farleigh and Racecourse mills in Queensland. Occurring just days into the 2026 crushing season, the incident has brought the regional agricultural supply chain to a complete standstill, halting not only sugar milling and cane haulage but also harvesting activities across approximately 1,300 predominantly family-owned farms. The company is currently working alongside specialized cybersecurity experts and relevant authorities to investigate the breach, secure their operational systems, and safely restore the affected infrastructure.

This incident strongly underscores the critical vulnerability of modern agricultural infrastructure, where Operational Technology (OT) and logistics systems are increasingly interconnected. The attack directly impacted the industrial perimeter, successfully penetrating or forcing the precautionary isolation of the utility's industrial control systems, which led to a complete halt of physical sugar milling and haulage processes. Because the mills' OT environment dictates the logistics of the entire harvesting schedule, the disruption triggered cascading effects, forcing growers to immediately cease harvesting activities and demonstrating how an industrial outage can paralyze an entire regional economy. Ultimately, this incident reflects a broader, dangerous trend identified by the Food and Ag-ISAC, which recently warned of sustained and sophisticated cyber pressure from threat actors actively targeting vulnerabilities within the farm-to-table supply chain.

The source is available at the following link:

Cyberattack disrupts Mackay Sugar operations, exposing growing agri-industrial cyber risks - Industrial Cyber

4. Book recommendation

Handbook on Operational Technology and its Security

This is a handbook aimed for professionals working in the Operational Technology (OT) area and Information Technology (IT) professionals working where IT is connected to OT, as well as top level management of organizations spanning both IT and OT environments. The handbook will provide an overview of the problems and possibilities when having connected IT and OT environments, as well as provide ideas and a potential structure for how this can be organized to achieve a risk-based approach for how to also include the OT and OT security alike IT and IT/information security in a minimalistic management system for IT/information/OT security. The reason to combine OT and OT security into a common framework is that these two are intricately intertwined due to the long lifecycles of OT assets and must be managed together for it all to work.

Author/Editor: John Lindström

Year of issue: 2025

The book is available and downloadable at the following link:

(PDF) Handbook on Operational Technology and its Security

5. Critical systems security news selection

Important articles dealing with critical infrastructure protection and industrial cybersecurity in June:

1. **Dragos Acquires Phosphorus to Bring OT-Native Cybersecurity to the Full xOT Environment**
2. **The Gentlemen ransomware combines advanced encryption with self-propagation, targeting critical sectors**
3. **Cyber adversaries shift from data theft to operational disruption as industrial crown jewels come under siege**
4. **CISA Urges OT Operators to Plan for Worst Case Scenarios**
5. **Exposed Fuel Tank Gauges Under Attack in the US**
6. **White House unveils AI security strategy focused on frontier models, cyber defense, critical infrastructure protection**
7. **Data Center OT Flaws Could Help Hackers Kill Power and AC**
8. **SANS expands Maryland cyber workforce program with new ICS/OT and AI security tracks, applications open**
9. **Resecurity details Anubis ransomware attack on Adriatic Port Authority, exposing maritime infrastructure risks**
10. **Mythos Shutdown Contains a Message: Don't Wait for Mythos**
11. **The checklist problem behind critical infrastructure cyber safety**
12. **Experts Warn of 'Mismatch' in US Response to OT Hacking**
13. **Data Foundation Drives Digital Success in Heavy Industry**
14. **Bridging the OT Cybersecurity Skills Gap**
15. **Asia-Pacific cyber threat environment intensifies as INTERPOL records surge in ransomware, phishing, DDoS attacks**
16. **Where IT meets OT and railway cybersecurity gets harder**
17. **Iran, Russia, China Target Water Systems for Sabotage**
18. **FDD's Ma warns weakening CISA could undermine US cyber resilience amid rising critical infrastructure threats**
19. **Forescout warns pre-disclosure exploitation of Lantronix flaw, mass OpenWrt targeting exposes OT edge security gaps**

Dragos Acquires Phosphorus to Bring OT-Native Cybersecurity to the Full xOT Environment

Dragos expands to protect xOT including OT systems and the billions of connected devices that have reshaped how critical infrastructure operates.

HANOVER, Md., June 1, 2026 — Dragos, the global leader in cybersecurity for operational technology (OT) environments, announced it has acquired Phosphorus, extending the Dragos Platform to protect the billions of connected devices embedded across critical infrastructure and other operational networks. …

Source and more information:

Dragos Acquires Phosphorus to Bring OT-Native Cybersecurity to the Full xOT Environment

The Gentlemen ransomware combines advanced encryption with self-propagation, targeting critical sectors

Microsoft Threat Intelligence detailed a growing RaaS (ransomware-as-a-service) operation known as The Gentlemen, tracked by Microsoft as Storm-2697, warning that the threat combines strong file encryption with aggressive self-propagation capabilities that can compromise entire enterprise networks. The analysis disclosed that the Go-based ransomware uses per-file ephemeral key encryption built on Curve25519 and XChaCha20, while simultaneously leveraging multiple lateral movement techniques to spread across connected systems, significantly increasing the speed and impact of attacks once initial access is obtained. …

Source and more information:

The Gentlemen ransomware combines advanced encryption with self-propagation, targeting critical sectors - Industrial Cyber

Cyber adversaries shift from data theft to operational disruption as industrial crown jewels come under siege

Protecting industrial crown jewels from espionage begins with recognizing a hard truth that in modern OT (operational technology) environments, the most critical assets are no longer merely physical systems. They make up an interconnected mix of control logic, operational data, and dependencies that sustain critical organizational operations. OT crown jewels have become prime cyber targets because they directly underpin national infrastructure such as energy, water, transport, and manufacturing. As systems converge with IT and cloud platforms, the attack surface expands, providing adversarial attackers with more access points into operational environments. …

Source and more information:

Cyber adversaries shift from data theft to operational disruption as industrial crown jewels come under siege - Industrial Cyber

CISA Urges OT Operators to Plan for Worst Case Scenarios

The latest initiative from the U.S. cyber defense agency aimed at operational technology operators is a little bit different. It's not advice about how to keep hackers out. It's not really about cybersecurity at all.

Instead, explained Cybersecurity and Infrastructure Security Agency ICS Cybersecurity Lead Matthew Rogers, CI Fortify is about what to do when cybersecurity fails.

"There's just a minimum of things that we can't really afford to have fail, at least for any sustained period of time," Rogers said, referring to the most vital sectors of critical infrastructure such as water and power. …

Source and more information:

CISA Urges OT Operators to Plan for Worst Case Scenarios

Exposed Fuel Tank Gauges Under Attack in the US

Cyberattackers are targeting Internet-exposed automatic tank gauge (ATG) systems in the United States, and the feds are urging site owners to take swift action.

ATGs are the electronic gauges that industrial sites use to monitor liquid storage tanks, whether they contain dangerous chemicals, fuel, or whatever else. Compared to some more elaborate machinery, they're rather straightforward things: probes that feed displays, which feed data to broader supervisory control and data acquisition (SCADA) systems so that plant operators can monitor their readings at a distance. Perhaps most folks give them little thought, especially in a cybersecurity context, but they're arguably as grave of a potential risk as any other equipment at any industrial facility anywhere. …

Source and more information:

Exposed Fuel Tank Gauges Under Attack in the US

White House unveils AI security strategy focused on frontier models, cyber defense, critical infrastructure protection

Following last week's release of an executive order aimed at strengthening the cybersecurity posture of government and private-sector systems in an era of increasingly advanced AI (artificial intelligence), the Executive Office of the President published a Federal Register notice directing federal agencies to work with the private sector to bolster the security of government and commercial information systems as AI capabilities become more widely deployed. …

Source and more information:

White House unveils AI security strategy focused on frontier models, cyber defense, critical infrastructure protection - Industrial Cyber

Data Center OT Flaws Could Help Hackers Kill Power and AC

Vulnerabilities in backup power devices and heating and cooling control systems widely used in data centers could enable remote cyberattacks by hackers and digital saboteurs and result in downtime and "devastating" operational impact, according to new research from operational technology security firm Claroty.

Claroty's Israel-based threat research team Team82, which presented its findings Tuesday at the SANS ICS Security Summit in Orlando, Fla., found two high-severity vulnerabilities in Vertiv's Liebert IS-UNITY-DP network cards, which provide connectivity for its uninterruptible power supply devices. Researchers also found five medium-severity vulnerabilities in the Trane Tracer SC+ HVAC controller. …

Source and more information:

Data Center OT Flaws Could Help Hackers Kill Power and AC

SANS expands Maryland cyber workforce program with new ICS/OT and AI security tracks, applications open

The SANS Cyber Workforce Academy has opened applications for an expanded Maryland training program that now includes dedicated ICS/OT and AI security tracks for career changers and IT professionals across the state. Applications opened on June 1 for the grant-funded initiative, which aims to help address growing cybersecurity workforce shortages. The expansion comes as the SANS 2026 Cybersecurity Workforce Research Report identifies the skills gap as the industry's leading workforce challenge, with 27% of organizations reporting that staffing shortages directly contributed to security breaches. …

Source and more information:

SANS expands Maryland cyber workforce program with new ICS/OT and AI security tracks, applications open - Industrial Cyber

Resecurity details Anubis ransomware attack on Adriatic Port Authority, exposing maritime infrastructure risks

New cyber threat intelligence from Resecurity provided further details on the Anubis ransomware group, which targeted the Adriatic Port Authority in a cyberattack that disrupted maritime logistics and exposed the growing risks facing critical transportation infrastructure. Hackers allegedly gained initial access through a spear-phishing email, then moved laterally across the network by exploiting unpatched vulnerabilities and escalating privileges. The attack encrypted systems supporting cargo tracking, shipping schedules, and customs processing and exfiltrated sensitive data, including contracts and employee records. …

Source and more information:

Resecurity details Anubis ransomware attack on Adriatic Port Authority, exposing maritime infrastructure risks - Industrial Cyber

Mythos Shutdown Contains a Message: Don't Wait for Mythos

The abrupt, government-ordered cut-off of access to Mythos 5, the most cyber-capable of Anthropic's large language models, has underlined a message security experts have been trying to get out to the operational technology community: You don't need Mythos.

"If there's any one message I've been trying to get out, it is, 'No, you don't have to wait to do this,'" said Patrick Miller, CEO of Ampyx Cyber, an OT security consulting firm.

Any of the commercially available large language models can be used to find vulnerabilities in software, Miller told ISMG in an interview. Mythos, and especially the latest version, Mythos 5, might be better at it than the others, but "pretty much any of these LLMs can do that fairly well," he said. ...

Source and more information:

Mythos Shutdown Contains a Message: Don't Wait for Mythos

The checklist problem behind critical infrastructure cyber safety

An asset owner can meet major federal cyber compliance standards and still run equipment that lacks the engineering to withstand an attack or a failure. New research from George Mason University examines how United States cyber policy defines reasonable care for systems that control physical processes, and it finds that compliance has become a stand-in for safety.

The work covers operational technology in critical infrastructure: industrial controls, medical devices, transportation systems, and building automation, where a software failure can produce physical harm. Its argument centers on a gap between data-centric IT security and the physics of the systems that policy now governs the same way. ...

Source and more information:

The checklist problem behind critical infrastructure cyber safety - Help Net Security

Experts Warn of 'Mismatch' in US Response to OT Hacking

A cyberattack of any significant scale against operational technology in America's vital infrastructure and services would almost immediately overwhelm the online and offline resources available to responders, experts said this week.

"We have a very large mismatch between expected capacity, expected demand, and current capacity," said Josh Corman, executive in residence for public safety and resilience at the Institute for Security and Technology. ...

Source and more information:

Experts Warn of 'Mismatch' in US Response to OT Hacking

Data Foundation Drives Digital Success in Heavy Industry

While heavy industrial organizations have invested excessively in dashboards and reporting tools, visibility alone is no longer enough. The next phase of digital transformation involves using data to generate predictive insights and prescriptive recommendations, said Abhisek Chakrabarti, head of digital programs at EET Fuels.

Many digital initiatives in the heavy industry fail because organizations focus on technology before addressing infrastructure readiness, data quality, business alignment and workforce adoption, Chakrabarti said. EET Fuels, formerly known as Essar Oil UK, is targeting a 90% reduction in carbon emissions at Stanlow Refinery, one of the U.K.'s largest refineries. The company has spent significant time strengthening its digital backbone, modernizing infrastructure, enhancing cybersecurity, consolidating applications and investing in data platforms such as Microsoft Fabric. ...

Source and more information:

Data Foundation Drives Digital Success in Heavy Industry

Bridging the OT Cybersecurity Skills Gap

The shortage of operational technology cybersecurity talent has evolved from a staffing challenge into a significant operational risk for critical infrastructure providers, said Dominic Grunden, CISO at Power and Water Corporation.

Grunden, a speaker at QG Media's OTsec ANZ Summit 2026 Sept. 15-16 in Sydney, said organizations that lack professionals who understand both OT and cybersecurity often struggle with slower vulnerability remediation, incomplete asset visibility and increased reliance on a small number of specialists. ...

Source and more information:

Bridging the OT Cybersecurity Skills Gap - OTToday

Asia-Pacific cyber threat environment intensifies as INTERPOL records surge in ransomware, phishing, DDoS attacks

New data from the INTERPOL warned that cybercrime is escalating sharply across Asia and the South Pacific, with its 2025/2026 Cyberthreat Assessment finding that cyber incidents now account for more than 30% of all recorded crime in over half of surveyed countries. The report, compiled using data from 18 member nations, links the surge to rapid digitalization, uneven cybersecurity maturity, and increasingly organized criminal networks exploiting expanding attack surfaces.

Phishing remains the most widespread and financially damaging threat, while ransomware, distributed denial-of-service (DDoS) attacks, AI-driven scams, and data breaches are rising in scale and sophistication. INTERPOL reported more than 135,000 ransomware-related attacks in 2024, a 92% jump in DDoS activity, and a 600% increase in deepfake-related discussions on cybercriminal forums, underscoring growing concerns over AI-enabled fraud and cross-border cybercrime operations targeting both consumers and critical sectors. …

Source and more information:

Asia-Pacific cyber threat environment intensifies as INTERPOL records surge in ransomware, phishing, DDoS attacks - Industrial Cyber

Where IT meets OT and railway cybersecurity gets harder

In this interview with Help Net Security, Jorge Aldegunde, Global Head of Railway Services at DNV, talks through what happens when old operational technology meets newer IT in monorail systems. He explains why open networks widened the attack surface, how teams decide whether to patch a signalling flaw without stopping trains, and who carries the liability.

Aldegunde covers regulation like CRA and NIS2, training veteran engineers to think about threat actors, and spotting intruders who have been inside for months. His main rule: manage your risks and plan for resilience, not perfection. …

Source (the interview) and more information:

Where IT meets OT and railway cybersecurity gets harder - Help Net Security

Iran, Russia, China Target Water Systems for Sabotage

Nation-state threat actors continue to attack systems that regulate, distribute, and protect water, but adversary objectives in these attacks can be more complex than they might first appear.

That's according to threat intelligence provider DomainTools, which on June 25 published research concerning recent nation-state targeting of water systems as far back as 2024. The research carried particular focus on how and why cyber adversaries are going after the infrastructure. …

Source (the interview) and more information:

Iran, Russia, China Target Water Systems for Sabotage

FDD's Ma warns weakening CISA could undermine US cyber resilience amid rising critical infrastructure threats

An executive at the Foundation for Defense of Democracies (FDD) warned that efforts to weaken or dismantle the U.S. CISA (Cybersecurity and Infrastructure Security Agency) could significantly undermine the nation's cyber resilience, arguing that the agency remains central

to defending critical infrastructure against escalating digital threats. In an analysis outlining five reasons CISA is indispensable, the report highlighted the agency's role in coordinating threat intelligence, securing federal networks, supporting incident response, protecting industrial and critical infrastructure systems, and strengthening public-private cyber collaboration, emphasizing that no other federal entity currently combines these capabilities at a comparable scale. …

Source (the interview) and more information:

FDD's Ma warns weakening CISA could undermine US cyber resilience amid rising critical infrastructure threats - Industrial Cyber

Forescout warns pre-disclosure exploitation of Lantronix flaw, mass OpenWrt targeting exposes OT edge security gaps

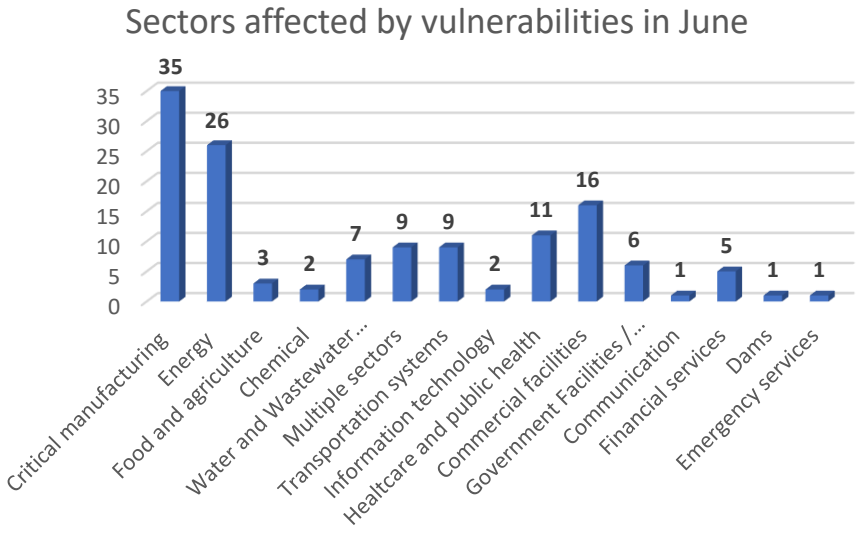
New analysis from Forescout Research – Vedere Labs revealed active exploitation of a critical vulnerability affecting Lantronix devices running modified OpenWrt LuCI interfaces, highlighting how attackers are weaponizing vendor patches before public disclosures are even released. The researchers observed exploitation attempts against CVE-2025-67038, an unauthenticated OS command injection flaw in Lantronix EDS5000 serial-to-IP converters, beginning after a patch became available but before Forescout published its technical findings, suggesting threat actors may have reverse-engineered the patch to develop working exploits. …

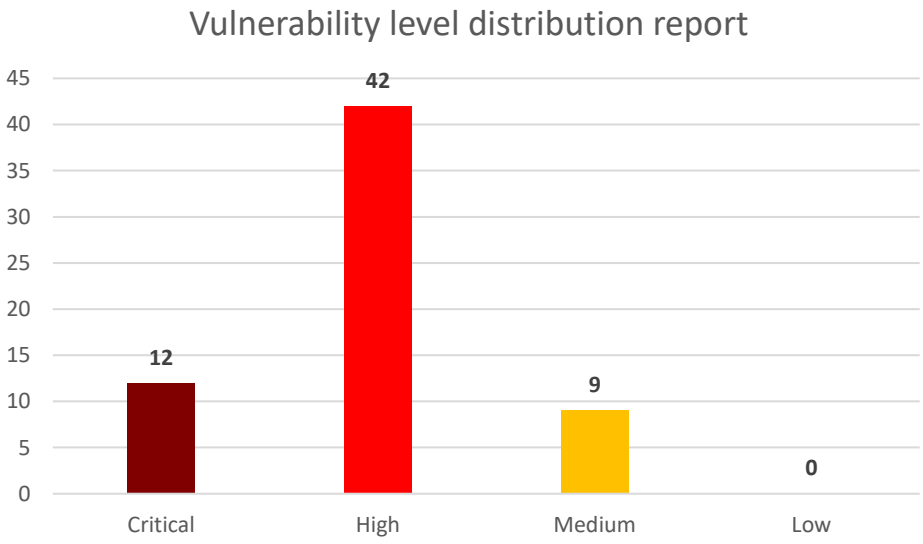
Source (the interview) and more information:

Forescout warns pre-disclosure exploitation of Lantronix flaw, mass OpenWrt targeting exposes OT edge security gaps - Industrial Cyber

6. Critical systems vulnerabilities

In June 2026, 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:





ICSMA-26-176-01: **pydicom pynetdicom Library**

Critical level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

pydicom pynetdicom Library | CISA

ICSMA-26-176-02: **OHIF Viewers DICOM**

High level vulnerability: Server-Side Request Forgery (SSRF).

OHIF Viewers DICOM | CISA

ICSA-26-176-01: **Yokogawa FAST/TOOLS and CI Server**

High level vulnerability: Cleartext Transmission of Sensitive Information.

Yokogawa FAST/TOOLS and CI Server | CISA

ICSA-26-176-02: **Evoke Systems**

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials.

EVoke Systems Charging Station Management System | CISA

ICSA-26-176-03: **Horner Automation Cscape**

High level vulnerability: Out-of-bounds Read.

Horner Automation Cscape | CISA

ICSA-26-176-04: **Daktronics Controller Firmware**

High level vulnerabilities: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Unrestricted Upload of File with Dangerous Type, Use of Hard-coded Credentials.

Daktronics Controller Firmware | CISA

ICSA-26-176-05: **H.VIEW HV-500S6 IP Camera**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Unrestricted Upload of File with Dangerous Type.

H.VIEW HV-500S6 IP Camera | CISA

ICSA-26-176-06: **Delta Electronics DTM Soft**

High level vulnerability: Deserialization of Untrusted Data.

Delta Electronics DTM Soft | CISA

ICSA-26-176-07: **Schneider Electric PowerLogic P7**

High level vulnerabilities: NULL Pointer Dereference, Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Reachable Assertion.

Schneider Electric PowerLogic P7 | CISA

ICSA-26-169-02: **AzeoTech DAQFactory (Update A)**

High level vulnerability: Access of Resource Using Incompatible Type ('Type Confusion'), Use After Free.

AzeoTech DAQFactory (Update A) | CISA

ICSA-26-174-01: **Siemens WinCC Certificate Manager**

High level vulnerability: Cleartext Storage in a File or on Disk.

Siemens WinCC Certificate Manager | CISA

ICSA-26-174-02: **Siemens SIPROTEC 5**

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

Siemens SIPROTEC 5 Using DIGSI5 Protocol | CISA

ICSA-26-174-03: **Siemens Products using OpenSSL**

Critical level vulnerability: Out-of-bounds Write.

Siemens Products using OpenSSL | CISA

ICSA-26-174-04: **Siemens SINEC INS**

High level vulnerabilities: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Path Traversal: '/dir/../filename', Execution with Unnecessary Privileges, Use of a One-Way Hash with a Predictable Salt.

Siemens SINEC INS | CISA

ICSA-26-174-05: **ABB Freelance Security Lock**

Medium level vulnerability: Authentication Bypass by Primary Weakness.

ABB Freelance Security Lock | CISA

ICSA-26-174-06: **Impact of Linux Kernel vulnerabilities on B&R products**

High level vulnerabilities: Incorrect Resource Transfer Between Spheres, Write-what-where Condition, Improper Privilege Management, Out-of-bounds Write, Multiple Releases of Same Resource or Handle.

Impact of Linux Kernel vulnerabilities on B&R products | CISA

ICSA-26-174-07: **Hubbell Aclara Metrum Cellular Web Interface**

High level vulnerability: Missing Authentication for Critical Function.

Hubbell Aclara Metrum Cellular Web Interface | CISA

ICSA-25-317-04: **Brightpick Mission Control / Internal Logic Control (Update A)**

High level vulnerabilities: Missing Authentication for Critical Function, Unprotected Transport of Credentials.

Brightpick Mission Control / Internal Logic Control (Update A) | CISA

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

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 C) | CISA

ICSA-26-111-06: **Zero Motorcycles Firmware (Update A)**

Medium level vulnerability: Key Exchange without Entity Authentication.

Zero Motorcycles Firmware (Update A) | CISA

ICSMA-26-169-01: **Apollo Pharmacy Blood Glucose Monitoring System APG-01 BT**

Medium level vulnerabilities: Cleartext Transmission of Sensitive Information, Missing Authorization.

Apollo Pharmacy Blood Glucose Monitoring System APG-01 BT | CISA

ICSA-26-169-01: **AVer PTC cameras**

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

AVer PTC cameras | CISA

ICSA-26-169-02: **AzeoTech DAQFactory**

High level vulnerability: Access of Resource Using Incompatible Type ('Type Confusion').

AzeoTech DAQFactory | CISA

ICSA-26-169-03: **Rockwell Automation FactoryTalk Historian Site Edition**

High level vulnerabilities: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), Uncaught Exception.

Rockwell Automation FactoryTalk Historian Site Edition | CISA

ICSA-26-169-04: **Schneider Electric EasyLogic T150 and Saitel DP**

High level vulnerability: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal').

Schneider Electric EasyLogic T150 and Saitel DP | CISA

ICSA-26-169-05: **Mitsubishi Electric MELSEC iQ-F Series**

High level vulnerability: Integer Overflow or Wraparound.

Mitsubishi Electric MELSEC iQ-F Series | CISA

ICSA-26-169-06: **Mitsubishi Electric Co.'s MELSEC iQ-F Series FX5-ENET/IP Ethernet Module**

High level vulnerability: Insufficient Entropy.

Schneider Electric Easergy, EcoStruxture, PowerLogic, and Saitel Products | CISA

ICSA-26-169-07: **Schneider Electric Easergy, EcoStruxture, PowerLogic, and Saitel Products**

High level vulnerability: Insufficient Entropy.

Schneider Electric Easergy, EcoStruxture, PowerLogic, and Saitel Products | CISA

ICSA-26-167-01: **Rockwell Automation FactoryTalk, Analytics, PavilionX**

High level vulnerability: Missing Authorization.

Rockwell Automation FactoryTalk Analytics PavilionX | CISA

ICSA-26-167-02: **Rockwell Automation RSLinx**

High level vulnerability: Out-of-bounds Read.

Rockwell Automation RSLinx | CISA

ICSA-26-167-03: **Rockwell Automation Logix 5370 & 5570 Controllers Vulnerable To Denial of Service Via CIP**

High level vulnerability: Improper Resource Shutdown or Release.

Rockwell Automation Logix 5370 & 5570 Controllers Vulnerable To Denial of Service Via CIP | CISA

ICSA-26-167-04: **Rockwell Automation CompactLogix**

High level vulnerabilities: Improper Validation of Integrity Check Value, Exposure of Sensitive System Information to an Unauthorized Control Sphere.

https://www.cisa.gov/news-events/ics-advisories/icsa-26-167-04

ICSA-26-167-05: **Rockwell Automation FLEX I/O EtherNet/IP Adapters**

Critical level vulnerabilities: Missing Release of Memory after Effective Lifetime, Missing Authentication for Critical Function.

Rockwell Automation FLEX I/O EtherNet/IP Adapters | CISA

ICSA-26-160-01: **Schneider Electric Modicon Network Managed Switches**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

Schneider Electric Modicon Network Managed Switches | CISA

ICSA-26-160-02: **Siemens KACO Blueplanet Inverters**

High level vulnerabilities: Use of Hard-coded Cryptographic Key, Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

Siemens KACO Blueplanet Inverters | CISA

ICSA-26-160-03: **Schneider Electric EcoStruxure Panel Server**

High level vulnerability: Initialization of a Resource with an Insecure Default.

Schneider Electric EcoStruxure Panel Server | CISA

ICSA-24-135-04: **Mitsubishi Electric Multiple FA Engineering Software Products (Update F)** **Medium** level vulnerabilities: Improper Privilege Management, Uncontrolled Resource Consumption, Out-of-bounds Write.

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

ICSA-24-326-03: **Schneider Electric Modicon M340, MC80, and Momentum Unity M1E & EcoStruxure (Update A)**

High level vulnerabilities: Improper Enforcement of Message Integrity During Transmission in a Communication Channel, Authentication Bypass by Spoofing.

Schneider Electric Modicon M340, MC80, and Momentum Unity M1E (Update A) | CISA

ICSA-25-035-06: **Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H (Update B)**

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

Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H (Update B) | CISA

ICSA-25-254-09: **Schneider Electric Modicon M340, BMXNOE0100, and BMXNOE0110 (Update A)**

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

Schneider Electric Modicon M340, BMXNOE0100, and BMXNOE0110 (Update A) | CISA

ICSA-26-162-01: **Yarbo Android/iOS Mobile Application and Cloud Infrastructure**

Critical level vulnerabilities: Use of Hard-coded Credentials, Missing Authorization.

Yarbo Android/iOS Mobile Application and Cloud Infrastructure | CISA

ICSA-26-162-02: **Naxclow IoT Platform**

Critical level vulnerabilities: Authorization Bypass Through User-Controlled Key, Missing Authorization, Not Using Password Aging, Use of Hard-coded Cryptographic Key, Generation of Predictable Numbers or Identifiers, Insertion of Sensitive Information into Externally-Accessible File or Directory.

Naxclow IoT Platform | CISA

ICSA-26-162-03: **Brickcom Cameras**

High level vulnerabilities: Missing Authentication for Critical Function, Use of Default Credentials.

Brickcom Cameras | CISA

ICSA-25-070-01: **Schneider Electric Uni-Telway Driver (Update D)**

Medium level vulnerability: Improper Input Validation.

Schneider Electric Uni-Telway Driver (Update D) | CISA

SSA-967325: **Multiple Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices (Update: 1.1.)**

Critical level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Reliance on Cookies without Validation and Integrity Checking, Server-Side Request Forgery (SSRF), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Check for Unusual or Exceptional Conditions, Heap-based Buffer Overflow, Improper Verification of Cryptographic Signature, Out-of-bounds Write.

SSA-967325

SSA-962515: **Out of Bounds Read Vulnerability in Industrial Products (Update: 1.6.)**

High level vulnerability: Out-of-bounds Read.

SSA-962515

SSA-870926: **Datakit and Parasolid Vulnerabilities in Simcenter Femap (Update: 1.1.)**

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

SSA-870926

SSA-864900: **Multiple Vulnerabilities in Fortigate NGFW on RUGGEDCOM APE1808 Devices (Update: 1.8.)**

High level vulnerabilities: Multiple.

SSA-864900

SSA-827968: **Vulnerability in Nozomi Guardian/CMC Before V26.2.0 on RUGGEDCOM APE1808 Devices (Update: 1.3.)**

High level vulnerabilities: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Incorrect Authorization, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements Used in a Template Engine.

SSA-827968

SSA-794185: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SIPROTEC, SICAM and Related Products (Update: 1.2.)**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-794185

SSA-723487: **RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products (Update: 2.0.)**

Critical level vulnerability: Improper Enforcement of Message Integrity During Transmission in a Communication Channel.

SSA-723487

SSA-722410: **Multiple Vulnerabilities in User Management Component (UMC) (Update: 1.2.)** **Critical** level vulnerabilities: Stack-based Buffer Overflow, Out-of-bounds Read.

SSA-722410

SSA-693808: **Deserialization Vulnerability in Siemens Engineering Platforms (Update: 1.3.)** **High** level vulnerability: Deserialization of Untrusted Data.

SSA-693808

SSA-674753: **Denial-of-Service Vulnerability in ET 200 Devices (Update: 1.2.)**

High level vulnerability: Uncontrolled Resource Consumption.

SSA-674753

ICSA-26-155-01: **NAVTOR NavBox**

Medium level vulnerability: Use of Hard-coded Credentials.

NAVTOR NavBox | CISA

ICSA-26-155-02: **Hitachi Energy ITT600 Explorer**

High level vulnerabilities: Uncontrolled Recursion, Allocation of Resources Without Limits or Throttling.

Hitachi Energy ITT600 Explorer | CISA

ICSA-26-155-03: **B&R PPT30 Operating System**

High level vulnerability: Allocation of Resources Without Limits or Throttling.

B&R PPT30 Operating System | CISA

ICSA-26-155-04: **Hitachi Energy RTU500**

High level vulnerabilities: NULL Pointer Dereference, Integer Overflow or Wraparound, Loop with Unreachable Exit Condition ('Infinite Loop').

Hitachi Energy RTU500 | CISA

ICSA-26-155-05: **Hitachi Energy MACH HiDraw**

Medium level vulnerability: Heap-based Buffer Overflow.

Hitachi Energy MACH HiDraw | CISA

ICSA-24-184-03: **Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update E)**

High level vulnerabilities: Allocation of Resources Without Limits or Throttling, Improper Verification of Cryptographic Signature, Uncontrolled Search Path Element, Missing Authentication for Critical Function, Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection').

Mitsubishi Electric Iconics Digital Solutions and Mitsubishi Electric Products (Update E) | CISA

ICSA-25-238-03: **Schneider Electric Modicon M340 Controller and Communication Modules (Update A)**

High level vulnerability: Improper Input Validation.

Schneider Electric Modicon M340 Controller and Communication Modules (Update A) | CISA

ICSA-25-219-06: **Dreame Technology iOS and Android Mobile Applications (Update A)**

High level vulnerability: Improper Certificate Validation.

Dreame Home iOS and Android Mobile Applications (Update A) | CISA

ICSA-25-079-01: **Schneider Electric EcoStruxure Process Expert (Update A)**

High level vulnerability: Improper Privilege Management.

Schneider Electric EcoStruxure (Update A) | CISA

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

ICS Advisories | CISA

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.

7. Critical systems security alerts

CISA has published alerts in 2026 June:

CISA Adds Known Exploited Vulnerabilities to Catalog

CVE-2024-21182 Oracle WebLogic Server Unspecified Vulnerability;
CVE-2022-0492 Linux Kernel Improper Authentication Vulnerability;
CVE-2025-48595 Android Framework Integer Overflow Vulnerability;
CVE-2026-45247 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data Vulnerability;
CVE-2026-28318 SolarWinds Serv-U Uncontrolled Resource Consumption Vulnerability;
CVE-2026-42271 BerriAI LiteLLM Command Injection Vulnerability;
CVE-2026-50751 Check Point Security Gateway Improper Authentication Vulnerability;
CVE-2026-7473 Arista Extensible Operating System Incomplete Comparison with Missing Factors Vulnerability;
CVE-2026-11645 Google Chromium V8 Out-of-Bounds Read and Write Vulnerability;
CVE-2026-20245 Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability;
CVE-2026-10520 Ivanti Sentry OS Command Injection Vulnerability;
CVE-2026-35273 Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability;
CVE-2026-20262 Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability;
CVE-2026-54420 LiteSpeed cPanel Plugin UNIX Symbolic Link (Symlink) Following Vulnerability;
CVE-2026-48907 Widget Factory Joomla Content Editor Improper Access Control Vulnerability;
CVE-2026-20253 Splunk Enterprise Missing Authentication for Critical Function Vulnerability;
CVE-2025-67038 Lantronix EDS5000 Code Injection Vulnerability;
CVE-2026-34908 Ubiquiti UniFi OS Improper Access Control Vulnerability;
CVE-2026-34909 Ubiquiti UniFi OS Path Traversal Vulnerability;
CVE-2026-34910 Ubiquiti UniFi OS Improper Input Validation Vulnerability;
CVE-2026-12569 PTC Windchill and FlexPLM Improper Input Validation Vulnerability;
CVE-2026-20230 Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability;
CVE-2026-48558 SimpleHelp Authentication Bypass Vulnerability;

Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA

CISA Adds Three 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 Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Four Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure
CISA is aware of global reports that malicious cyber actors have targeted internet-accessible Fortinet devices across government and private sector organizations using compromised credentials. This activity, referred to as FortiBleed, involves the exposure of leaked credentials associated with approximately 74,000 Fortinet devices, including firewalls and virtual private network (VPN) gateways.
Links and more information:
CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure | CISA

8. Critical systems security trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in July 2026:

- Internet of Things (IoT) Practitioner (Exam ITP-110)
- Internet of Things (IoT) Security (Exam ITS-110)

Coursera | Online Courses From Top Universities. Join for Free

- Industrial Control Systems Cybersecurity (Virtual)(ICS300)
- Industrial Control Systems Evaluation (Virtual)(401V)
- ICS Cybersecurity & RED-BLUE Exercise (In-Person)(ICS301)
- Industrial Control Systems Evaluation (In-Person)(401L)
- Introduction to Control Systems Cybersecurity (In-Person)(101)
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)

ICS Training Available Through CISA | CISA

- 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

ICS410: ICS/SCADA Security Essentials | SANS Institute

- ICS/SCADA Cyber Security
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

ICS/SCADA Cyber Security

- SCADA security training

SCADA Security Training | SCADA Security Training Course

- 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

ICSP Training Boot Camp (OT/ICS Certified Security Professional) | Infosec

- Industrial Control System (ICS) & SCADA Cyber Security Training

Industrial Control System and SCADA Cybersecurity Training - Tonex Training

- Bsigroup: Certified Lead SCADA Security Professional training course

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

- The Industrial Cyber Security Certification Course

Certified Industrial Cybersecurity Professional Certification | CICP Course

- Secure IACS by ISA-IEC 62443 Standard

Secure IACS by ISA-IEC 62443 Standard

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

ISA/IEC 62443 Training for Product and System Manufacturers | UL Solutions

- ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

- ICS/OT Cyber ICS/OT Cybersecurity as per NIST 800-82 Updated - Part1

ICS/OT Cybersecurity as per NIST 800-82 Updated - Part1

- Lead SCADA Security Manager

Lead SCADA Security Manager | PECB

- OT/IT Security Training

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

- OT Railway Cybersecurity (OTCS)

OT Railway Cybersecurity (OTCS) Training - Informa Academy

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

OT Security Expert - OPSWAT Academy

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

CTR-008 - OT-Security Awareness E-Learning Course | Yokogawa Europe

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

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

- Cybersecurity for Industrial Automation (ICS/SCADA) and OT

https://www.imfacademy.com/security-management/ot-cybersecurity.php

9. Critical systems security 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.

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/