Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 05, 2026

Smart Brevity® count: 4.5 mins...1187 words

This issue brings you the latest developments in cybersecurity threats, underscoring the ongoing need for vigilance.

CISA Releases Five Industrial Control Systems Advisories

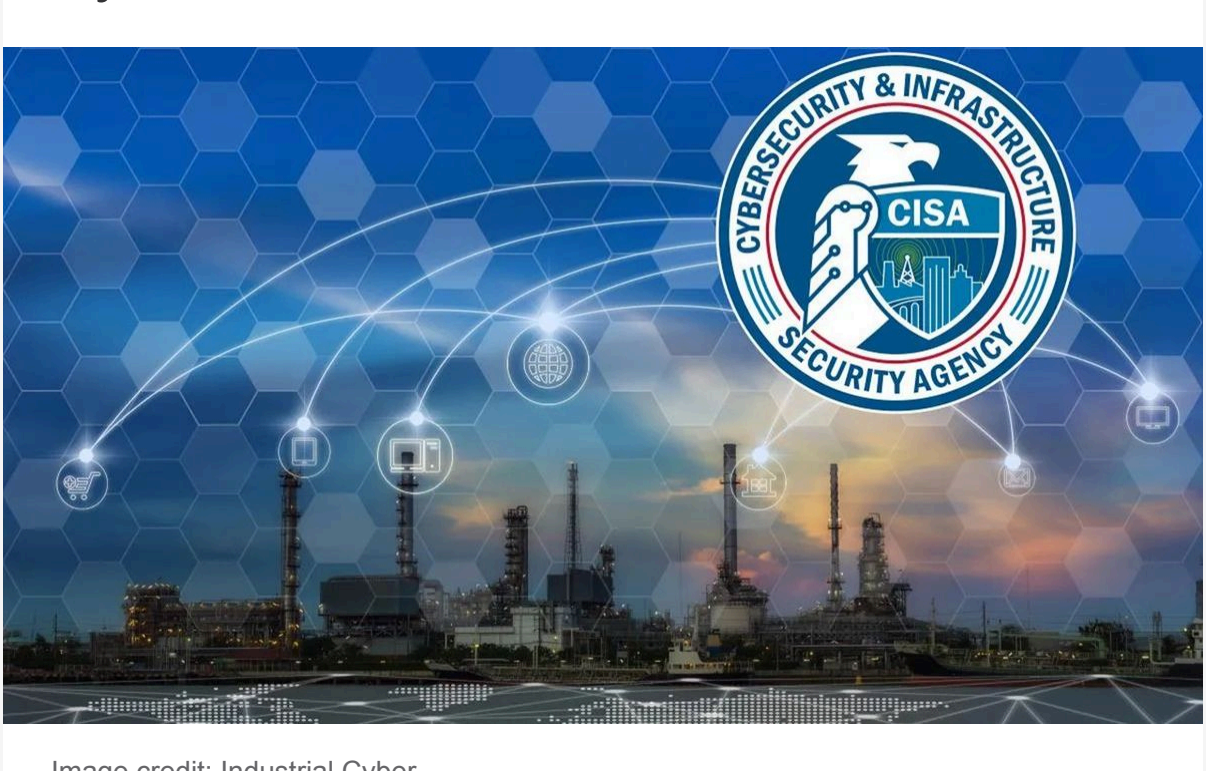

Image credit: Industrial Cyber

5 June 2026

CISA released five Industrial Control Systems (ICS) Advisories. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

- ICSA-26-155-01 NAVTOR NavBox
- ICSA-26-155-02 Hitachi Energy ITT600 Explorer
- ICSA-26-155-03 B&R PPT30 Operating System
- ICSA-26-155-04 Hitachi Energy RTU500
- ICSA-26-155-05 Hitachi Energy MACH HiDraw

CISA encourages users and administrators to review newly released ICS Advisories for technical details and mitigations.

Read full article here

Cisco warns of critical Unified CM flaw

Image credit: Cisco

4 June 2026

Cisco has released updates to patch a critical Unified Communications Manager (Unified CM) flaw that allows attackers to gain root privileges.

Why it matters: This vulnerability could let attackers elevate their privileges to root, posing a significant risk to organizations using Cisco's IP telephony systems.

- The flaw, tracked as CVE-2026-20230, can be exploited remotely without privileges.
- Cisco's PSIRT team is aware of publicly available exploit code but has not found active exploitation.

Details: This vulnerability affects systems with the WebDialer service enabled; however, it is disabled by default.

- Administrators should check the WebDialer status via the Cisco Unified CM Administration interface.
- To mitigate risks, install Cisco Unified CM versions 14SU6 or 15SU5, or disable WebDialer temporarily.

What's next: Cisco urges immediate patch installation and has provided detailed steps to disable WebDialer.

- In January, Cisco fixed another critical vulnerability (CVE-2026-20045) actively exploited as a zero-day.
- The U.S. Cybersecurity and Infrastructure Security Agency has tagged numerous Cisco vulnerabilities as actively exploited over the past years.

Read full article here

Microsoft resolved caching issue from unexpected Windows driver updates

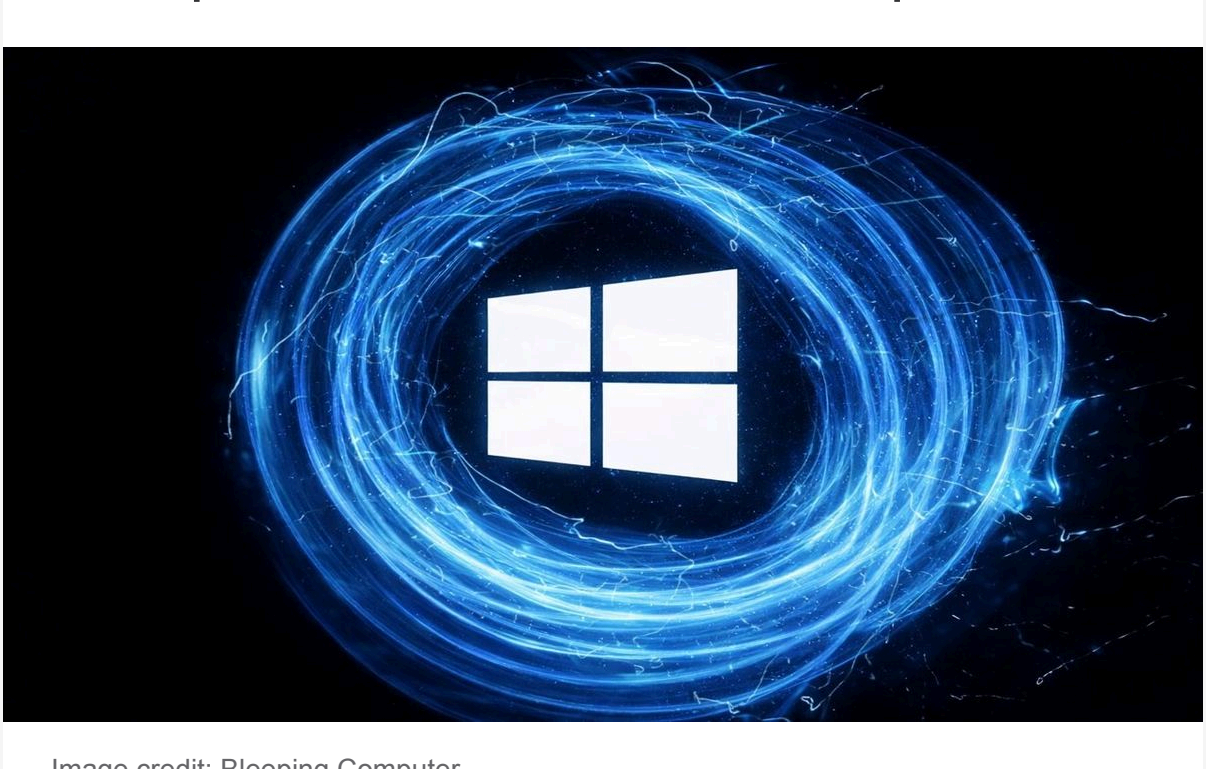

Image credit: Bleeping Computer

4 June 2026

Microsoft resolved an issue causing unexpected driver updates on Windows devices, despite configured policies to prevent them.

Why it matters: The misconfiguration affected device enrollment information, leading to unauthorized driver installations, posing challenges for IT admins.

- Microsoft confirmed the updates were approved and posed no security threat.

What they're saying: Microsoft's Intune Support Team acknowledged the issue on Twitter and Reddit, assuring active work to mitigate the problem.

- "The drivers being installed are Microsoft approved/signed," Microsoft stated, confirming no security threat.

The latest: Microsoft has updated the service cache and enrollment status, confirming issue resolution.

- The company is reviewing the incident to improve future detection and prevention.

The backdrop: Past issues include unexpected upgrades on Windows Server systems and driver updates on Windows 11 devices in the EU, highlighting ongoing challenges in update management.

Read full article here

New IronWorm malware hits 36 npm packages in supply-chain attack

Image credit: Bleeping Computer

4 June 2026

IronWorm malware was used in a new supply-chain attack targeting 36 npm packages aiming to steal sensitive credentials.

Why it matters: This attack highlights vulnerabilities in the npm ecosystem, risking exposure of critical credentials like OpenAI, AWS, and cryptocurrency wallet files.

- The malware's Rust-based design and eBPF rootkit make it harder to detect.
- Its propagation through npm's Trusted Publishing workflow amplifies the threat.

The big picture: While no clear link to Shai Hulud was found, similarities suggest IronWorm could be its evolution.

- JFrog's findings indicate the attack's intricate design to evade detection, using GitHub Actions for secret delivery.

What's next: Developers are urged to upgrade packages, rotate keys, and enable 2FA to safeguard against similar threats.

- Companies like Ox Security emphasize early detection as a key defense strategy.

Read full article here

FlutterShell backdoor targets macOS

Image credit: Bleeping Computer

4 June 2026

Cybersecurity researchers have uncovered a macOS malvertising campaign, Operation FlutterBridge, spreading a new backdoor named **FlutterShell**.

Why it matters: FlutterShell poses a significant threat as it infects users with adware and has backdoor capabilities.

- This affects macOS users in the U.S., Canada, Australia, France, and Germany.
- The campaign uses malicious desktop applications built with the Flutter framework.

Driving the news: CL-CRI-1089, the cybercrime group behind this, has been active since 2023 and also conducting operations like Recipe Lister and Calendaromatic.

- These campaigns involve trojanized software to deliver potentially unwanted programs.
- Front companies like AdsParkPro LTD play a role in distributing malicious Google and YouTube ads.

Bottom line: FlutterShell's WebView-based architecture allows dynamic behavior changes, enabling attackers to host malicious logic externally.

- This technique bypasses the need for recompilation of malware, evading Apple security checks.
- Variants like PodcastsLounge and PDF-Ninja highlight its ongoing development and sophistication.
- The rapid development and delivery of new FlutterShell variants, indicates this campaign is just beginning.

Read full article here

Police dismantle fake ID marketplace used by migrant smugglers

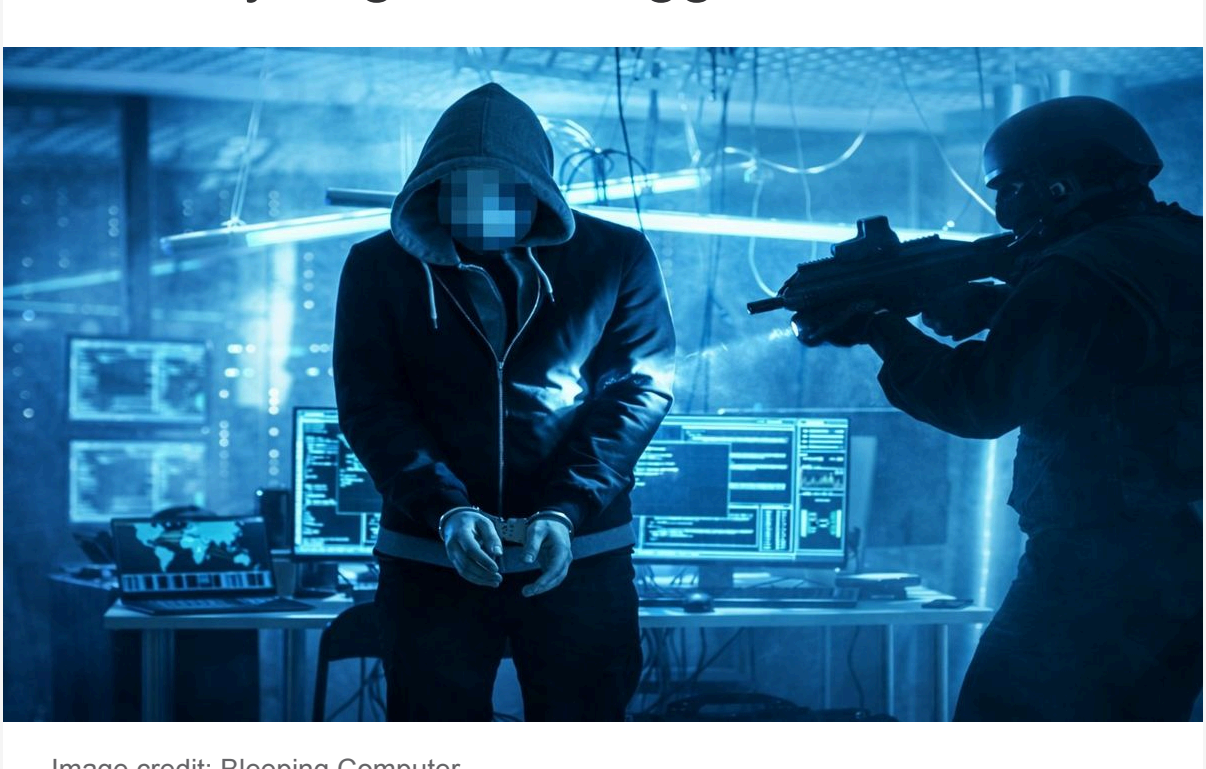

Image credit: Bleeping Computer

4 June 2026

French and Spanish authorities took down an online marketplace selling fake identity documents to migrant smuggling rings within the EU.

Why it matters: This crackdown disrupts a key enabler of migrant smuggling, hindering criminal networks' ability to evade border controls.

- The operation seized 800 counterfeit IDs and document-production equipment.
- It highlights the ongoing threat posed by document fraud in facilitating illegal activities.

The big picture: Europol has expanded its anti-smuggling efforts, establishing the European Centre Against Migrant Smuggling (ECAMS) to bolster intelligence sharing and financial investigations.

Go deeper: Europol's 2025 EU Serious and Organized Crime Threat Assessment flagged document fraud as a major enabler of smuggling, underscoring the need for enhanced collaborative efforts across agencies.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

Lazarus Group Uses npm Brandjacking Campaign to Target Developers

Payouts King Ransomware Evades EDR with Obfuscation and Direct System Calls

Hackers Spied on a Stock Exchange Executive's Outlook Mailbox for 5 Months

Credit card theft campaign abuses Stripe to host stolen payment info

DentaQuest data breach exposed info of 2.6 million accounts

Ultrahuman data breach exposes user info via internal tool

Russia seeks to label two anti-Kremlin hacker groups as extremist

UN food agency investigates breach exposing data of Gaza aid recipients

Critical Vulnerabilities

Researcher publishes GitHub token-stealing exploit

Acer Working to Patch Wave 7 Router 0-day Vulnerability

Everest Forms Pro Vulnerability Allows Remote Code Execution on WordPress Sites

Teams and Google Drive Leveraged to Compromise Systems

Hackers Use Fake Chrome Web Store Copyright Notices to Steal Google Credentials

Mitigation

How Proton Mail Fights Against Cybercriminals Using Its Services

DoJ Disrupts Southeast Asia Fraud Networks, Freezes $3.8 Million in Assets

Cyber Studies

Bots Surpass Humans in Global Web Traffic for the First Time

Inside the race to adapt to an AI-powered security world

Hackers Are After Gaps in Your Vulnerability Program: Here's Their Playbook

Latest cybersecurity advisories and notices

Image credit: IoT World Today

Latest CISA cybersecurity and advisories here.

Latest Microsoft security updates here.

Latest Drupal security advisories here.

Latest CISCO security advisories here.

Latest SUSE security advisories here.

Latest UBUNTU security notices here.

Latest Checkpoint advisories here.

Latest Red Hat product Errata notices here.

Latest zero-day initiative advisories here.

.

NOT FOR PUBLIC DISSEMINATION

TSA Transportation Security Operations Center 866- 615- 5150 and TSOC.ST@tsa.dhs.gov

For questions regarding this product and/or if you know someone interested in joining and receiving this product contact the PT-ISAC at PT-ISAC@APTA.com.

Disclaimer: This product contains news articles compiled from open-source and commercially available information. Information contained is for situational awareness only and does not represent the views of the PT ISAC. Only the analyst comments represent the views of the PT-ISAC.