Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 12, 2026

Smart Brevity® count: 5 mins...1265 words

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

CISA Adds One Known Exploited Vulnerability to Catalog

Image credit: Cybercory

12 June 2026

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2026-10520 Ivanti Sentry OS Command Injection Vulnerability

This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Binding Operational Directive (BOD) 26-04: Prioritizing Security Updates Based on Risk establishes vulnerability management requirements for Federal Civilian Executive Branch (FCEB) agencies, updating BOD 22-01. BOD 26-04 reinforces the importance of the KEV catalog and requires federal agencies to prioritize rapid remediation of high-risk vulnerabilities, specifically those identified by Common Vulnerabilities and Exposures (CVEs) listed in CISA's Known Exploited Vulnerabilities (KEV) catalog on publicly exposed assets that grant total control of the asset post-exploitation, while deferring action for lower-risk vulnerabilities. BOD 26-04 further establishes basic expectations for when agencies must check whether threat actors compromised the system before the patch was applied.

While BOD 26-04 applies only to FCEB agencies, CISA encourages all organizations to adopt risk-based vulnerability management and prioritize remediation of KEV catalog vulnerabilities. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

Read full article here

CISA Releases Three Industrial Control Systems Advisories

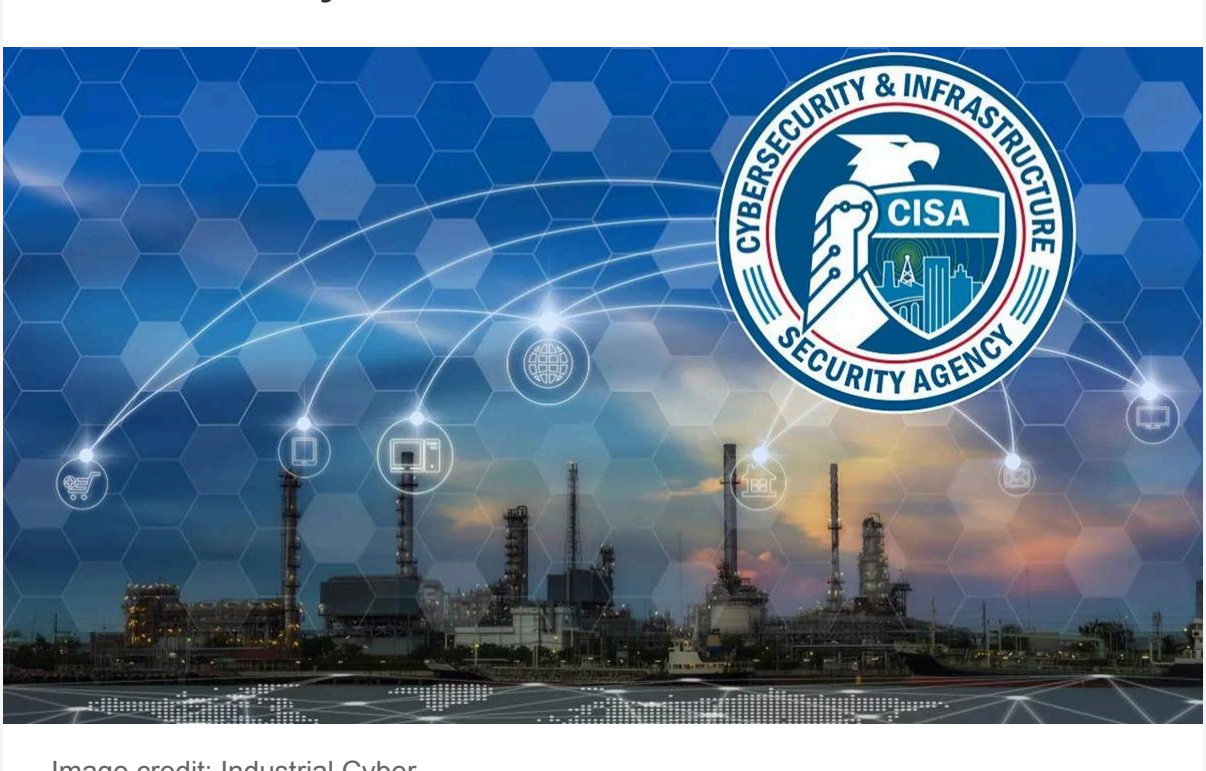

Image credit: Industrial Cyber

11 June 2026

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

- ICSA-26-013-01 Yarbo Android/iOS Mobile Application and Cloud Infrastructure
- ICSA-26-013-02 Naxclow IoT Platform
- ICSA-26-013-03 Brickcom Cameras

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

Read full article here

The Gentlemen Ransomware claims 478 victims, can spread like a worm

Image credit: LinkedIn

11 June 2026

The Gentlemen ransomware has struck 478 victims, leveraging worm-like propagation tactics to increase its reach.

Why it matters: This rapid spread raises alarms for cybersecurity experts worldwide as it targets a wide range of sectors.

- Organizations must bolster defenses against this evolving threat, especially those vulnerable to sophisticated ransomware campaigns.
- The group's integration of AI in developing and maintaining its tools complicates mitigation efforts.

Details: Initially part of Phantom Mantis, The Gentlemen now operates independently, enticing affiliates with a lucrative profit-sharing model.

- The mastermind, LARVA-368, utilizes AI for strategic development and post-exploitation procedures.
- The ransomware's evolution includes adapting and changing tactics during attacks, making it a formidable adversary.

What's next: Security professionals need to stay vigilant and innovative in countering The Gentlemen's tactics.

- Updating and strengthening cybersecurity measures is crucial to prevent further exploitations.

Read full article here

Interpol dismantles SniperDz Phishing-as-a-Service platform

Image credit: Interpol

11 June 2026

Interpol, in collaboration with cybersecurity firm Group-IB, has successfully taken down the SniperDz phishing-as-a-service platform and arrested its main operator.

Why it matters: This operation, known as Operation Ramz, marks a significant step in combating global cybercrime impacting phishing operations.

- The crackdown resulted in 201 arrests, seizure of 53 servers, and identification of 382 suspects and 3,867 victims.

SniperDz's global reach: Since 2015, SniperDz has offered phishing kits and operational support to cybercriminals worldwide.

- Palo Alto Networks previously linked over 140,000 phishing pages to SniperDz.
- Group-IB discovered 20,000 domains impersonating major organizations like PayPal and Netflix.

OpSec failures exposed: The investigation uncovered significant operational security lapses by the suspect.

- Video tutorials and social media activity helped trace the suspect's digital footprint.
- Evidence included a Telegram channel with over 7,300 subscribers and a Facebook account followed by more than 19,000 users.

Bottom line: The operation underlines the importance of adversary-centric intelligence and collaboration among industry and law enforcement.

Read full article here

Hacker linked to Void Blizzard faces charges for cyberespionage campaign

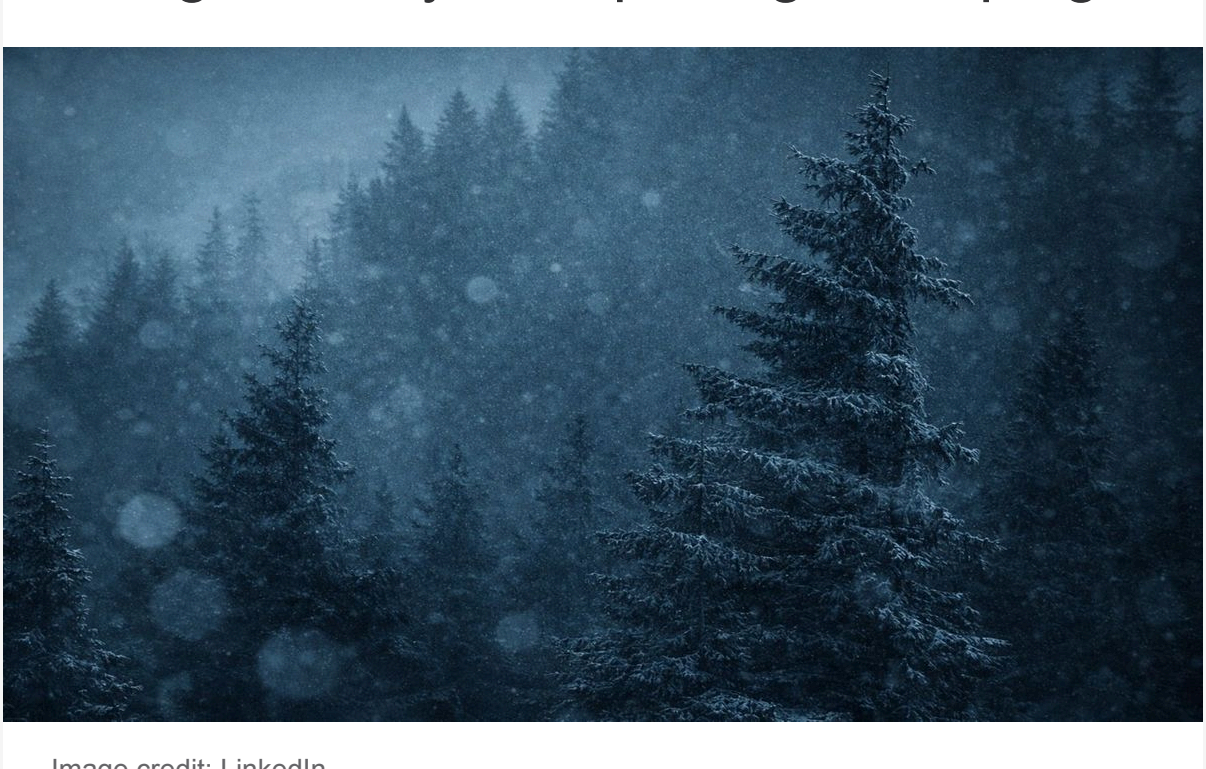

Image credit: LinkedIn

11 June 2026

A Russian national with links to the Void Blizzard hacking group appeared in U.S. federal court this week on charges of supporting a Kremlin-linked cyberespionage campaign targeting U.S. companies.

Why it matters: The case highlights the ongoing threat of cyberespionage and the international cooperation required to address it.

- Denis Obrezko, 36, was transferred to U.S. custody from Thailand and is accused of providing infrastructure for Void Blizzard's operations.
- Prosecutors allege cryptocurrency transactions linked to Obrezko facilitated attacks against U.S. organizations.

The big picture: Void Blizzard is a relatively new threat group aligned with Russian interests, targeting various sectors across Europe and North America.

- Investigators have identified at least 11 U.S. companies compromised, with the actual number believed to be higher.

What's next: Obrezko remains in custody as the case proceeds, with Russian diplomats seeking his return and Moscow placing him on an international wanted list.

Read full article here

Siemens patch erroneously flagged as malware by cybersecurity solutions

Image credit: Siemens

11 June 2026

Siemens alerts customers that patch files for its Desigo CC building management system are mistakenly being flagged as malware by several cybersecurity solutions.

- **Desigo CC integrates** HVAC, lighting, security, fire safety, power, and other building subsystems into a unified platform for centralized control and monitoring.
- **Recent discovery:** Patch files for versions 7 through 9 are being detected as malicious by various antivirus engines, as confirmed by tests on VirusTotal.

Why it matters: Siemens is collaborating with cybersecurity vendors to fix the file classification inaccuracies, suspecting that a PowerShell script compiled as an executable is the root cause.

- **Script details:** The 'patchHelper' script within Desigo CC patches performs file system operations, registry modifications, and executes with elevated privileges, triggering suspicion among security engines.

Interesting note: The script has been consistent for months but is only now receiving malware flags.

- Siemens verified all relevant files against development repositories, finding no discrepancies or malicious modifications. Additionally, digital signatures were validated as genuine with no signs of tampering.

Background: This is not Siemens' first encounter with challenges from third-party cybersecurity solutions. Last year, issues with Microsoft Defender Antivirus affecting its Simatic PCS products were reported.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

BLUERABBIT Backdoor Encrypts Files, Wipes Disks on Windows Systems

OnyxC2 stealer offers cybercriminals enterprise-grade theft for $250 a month

Hackers Abuse Residential Proxy Networks to Hide Malicious Activity and Evade Detection

Maine breach portal abused to publish fake data breach disclosures

Handala Claims Breach of California Water Service

University of Nottingham confirms cyber incident as Shiny Hunters group claims data theft

OceanLotus Hits Vietnam Investors With SPECTRALVIPER in FireAnt Attack

Critical Vulnerabilities

Microsoft fixes BitLocker recovery bug on Windows Server 2025

Chrome update will soon disable adblockers

New Attacks Trick OpenClaw AI Agent into Running Code, Leaking Secrets

Hackers Exploit Langflow Vulnerability for Remote Code Execution

Mitigation

Oracle mitigates PeopleSoft zero-day exploited in data theft attacks

Authorities dismantle 'AudiA6' ransomware crypto-laundering service

Cyber Studies

Alert Fatigue Is Becoming a Security Threat of Its Own

Extortion-Only Attacks Increase, Data Theft Dominating Ransomware Claims

Phishing Attack Volume Down 20%, but Risk Still Rising

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.