Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 16, 2026

Smart Brevity® count: 5 mins...1389 words

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

CISA Adds Two Known Exploited Vulnerabilities to Catalog

Image credit: Cybercory

16 June 2026

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

- 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

These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose 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

New analysis of ransomware attack on Italian Adriatic Port Authority

Autorità di Sistema Portuale del Mar Adriatico Centrale

Porti di Pesaro, Falconara, Ancona, S. Benedetto, Pescara, Ortona, Vasto

Image credit: Adriatic Port Authority

15 June 2026

Anubis ransomware group attacked the Adriatic Port Authority, highlighting vulnerabilities in maritime infrastructure according to a new Resecurity analysis of the attack.

- The original breach occurred on December 11, 2025.

Why it matters: This incident underscores the growing threat of ransomware on critical infrastructure, with significant implications for maritime security.

- The attack compromised 2% of the port's data, including sensitive safety plans and security operations.
- Resecurity reports a $10m Bitcoin ransom demand, with operations severely disrupted and vessels rerouted.

The big picture: Anubis, known for its ransomware-as-a-service model, offers lucrative incentives to affiliates, contributing to its widespread impact across various sectors.

- The group exploits vulnerabilities in systems like SonicWall VPNs and SolarWinds Web Help Desk.

What's next: The maritime sector must enhance cybersecurity defenses to mitigate such threats as digitization increases the attack surface.

- The attack further highlights the focus of ransomware groups on critical infrastructure including transportation infrastructure.
- Resecurity warns that outdated IT systems and low cyber maturity leave the maritime sector vulnerable to future attacks.

Read full article here

China espionage group lurking in networks undetected since 2023

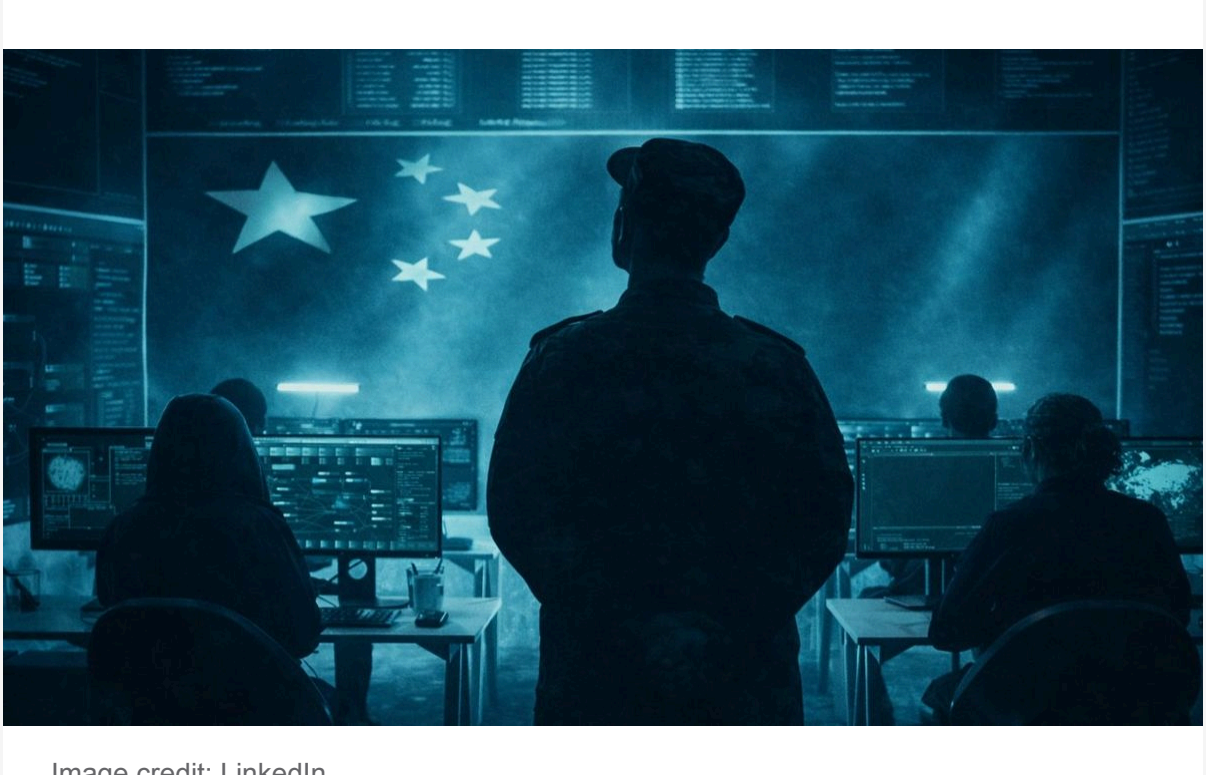

Image credit: LinkedIn

15 June 2026

Google's Threat Intelligence Group uncovered a new Chinese espionage group, UNC6508, which has infiltrated U.S. and Canadian entities since 2023.

Why it matters: This group has targeted sectors with national security implications, using advanced techniques to remain undetected.

- They exploited REDCap servers, a tool employed widely in medical research, to steal data.
- The campaign demonstrates China's continued cyber threats against defense, technology, and medical industries.

The big picture: The group's actions align with a broader pattern of Chinese state-backed cyber-espionage.

- UNC6508's stealth operations included abusing domain compliance rules and routing traffic through U.S.-based IPs.
- The group remains active, prompting ongoing investigations into potential compromises.

What's next: Google has disrupted some of the group's infrastructure and continues to support affected organizations in remediation efforts.

- Several unconfirmed breaches remain under investigation, highlighting the persistent threat from UNC6508.

Read full article here

Palo Alto warns of GlobalProtect VPN vulnerability exploited in the wild

Image credit: Palo Alto Networks

15 June 2026

Palo Alto Networks Unit 42 has issued an urgent warning about active exploitation of CVE-2026-0257, a critical authentication bypass vulnerability in the GlobalProtect portal and gateway components of PAN-OS software.

Why it matters: This flaw allows unauthenticated remote attackers to initiate unauthorized VPN connections without credentials, posing a significant security threat.

- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to its Known Exploited Vulnerabilities (KEV) catalog due to its severity.

The latest: Unit 42 researchers have identified an unknown threat actor actively probing GlobalProtect-enabled devices, with a few targets establishing actual VPN sessions.

- No post-access behavior or data exfiltration has been confirmed yet, but the risk persists.

Action steps: Organizations should immediately review their GlobalProtect logs for indicators of compromise and activate incident response protocols.

- GlobalProtect: Indicators of Compromise.
- Refer to the official Palo Alto Networks security advisory and apply available workarounds or upgrade to a patched PAN-OS version.
- Rapid7 has also published a technical analysis of the activity in the wild.

What's next: Threat hunters should search GlobalProtect logs for successful login connections from specific IP addresses, especially for activity predating the public PoC release on May 29, 2026.

Read full article here

Cisco fixes SD-WAN vManage flaw exploited in zero-day attacks

CISCO

Image credit: Cisco

15 June 2026

Cisco has released a fix for a vulnerability in its Catalyst SD-WAN Manager, previously known as SD-WAN vManage.

Why it matters: The flaw allowed attackers to escalate privileges to root, affecting all deployment types including on-prem and cloud-managed systems.

- Insufficient validation during file uploads could let low-privilege attackers execute commands as root.
- Cisco's Product Security Incident Response Team (PSIRT) urges immediate patching.

The latest: In recent months, multiple vulnerabilities in Cisco's SD-WAN solutions have been flagged as exploited in the wild.

- February saw an information disclosure flaw actively exploited (CVE-2026-20133).
- Last month, a maximum-severity flaw was highlighted for authentication bypass (CVE-2026-20182).
- In early June, another zero-day was flagged, allowing root access (CVE-2026-20245).

What's next: Administrators should check their SD-WAN vmanage-server, vmanage-appserver, and serviceproxy-access logs for attempts to upload index.jsp and .war files as indicators of compromise.

Read full article here

New attack turned Microsoft 365 Copilot into 1-click data theft tool

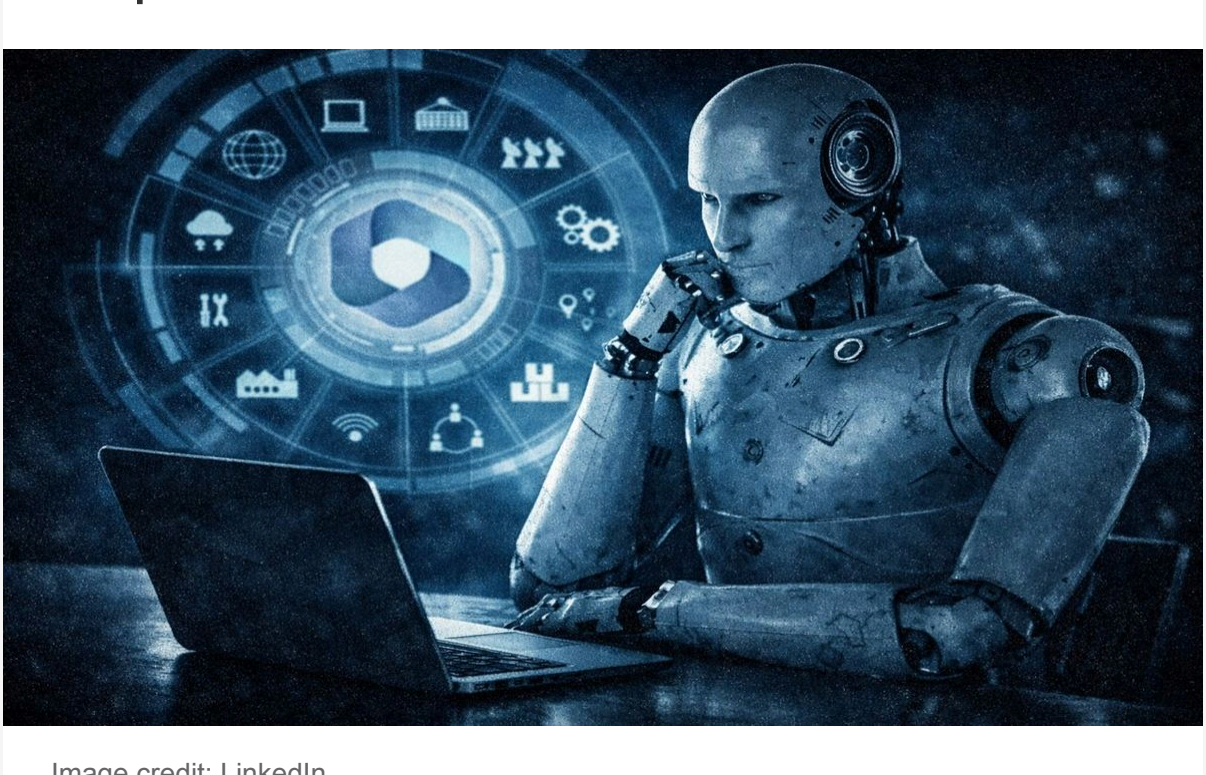

Image credit: LinkedIn

15 June 2026

A critical vulnerability named SearchLeak in Microsoft 365 Copilot Enterprise has been identified, allowing potential data theft through a specially crafted URL.

Why it matters: This flaw could expose sensitive data from mailboxes, OneDrive, or SharePoint accounts, posing a significant risk to security.

- Attackers can exploit this vulnerability to access email content, calendar events, and documents.
- The vulnerability was assigned the CVE-2026-42824 identifier with a critical rating.

Attack details: Researchers at Varonis discovered the attack chain by combining three weaknesses: parameter-to-prompt injection, HTML rendering race condition, and SSRF in Bing's feature.

- It begins with a crafted URL that initiates a search in Copilot without user input.
- The attack leverages an HTML rendering glitch to execute unauthorized requests.

Resolution: Microsoft has addressed the vulnerability, ensuring no user action is needed for mitigation.

- Familiar bugs, when combined with AI, can create new attack vectors, highlighting the evolving nature of cyber threats.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

North Korean Hackers Are Turning Developer Tools into Malware Delivery Channels

Sysco hit by ShinyHunters extortion, weeks after Qilin ransomware threat

ShinyHunters claims Kodak hack, threatens to leak 2.2M records

Hackers demand $2M from Nintendo over alleged data breach

Belarus-linked hackers target Gmail accounts of Polish public figures and their families

FBI PSA: Scammers Use Couriers to Collect Cash in Cryptocurrency Investment Scams

Critical Vulnerabilities

LiteLLM Vulnerability Chain Lets Low-Privilege Users Take Over AI Gateway Servers

Windows 11 Update KB5094126 Freezes Systems, Forces BitLocker Recovery

SimpleHelp bug lets hackers create rogue remote support accounts

OptinMonster WordPress plugin hacked in CDN supply-chain attack

Over 50 Android Apps Found Spreading MagicAd Trojan via Official Stores

Mitigation

US Cracks Down on Anthropic AI Models Amid Abuse Concerns

Anthropic Updated Privacy Policy to Include Identity Verification for Claude Users

Cyber Studies

Inside the Modern SOC: The 72-Minute Race

Is it possible to build a fully autonomous SOC?

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.