Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 10, 2026

Smart Brevity® count: 5 mins...1333 words

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

CISA Adds Three Known Exploited Vulnerabilities to Catalog

Image credit: Cybercory

10 June 2026

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

- 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

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) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of KEV Catalog vulnerabilities as part of their vulnerability management practice. 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

9 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-26-160-01 Schneider Electric Modicon Network Managed Switches
- ICSA-26-160-02 Siemens KACO Blueplanet Inverters
- ICSA-26-160-03 Schneider Electric EcoStruxure Panel Server

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

Read full article here

Microsoft breaks Patch Tuesday record with 206 vulnerabilities

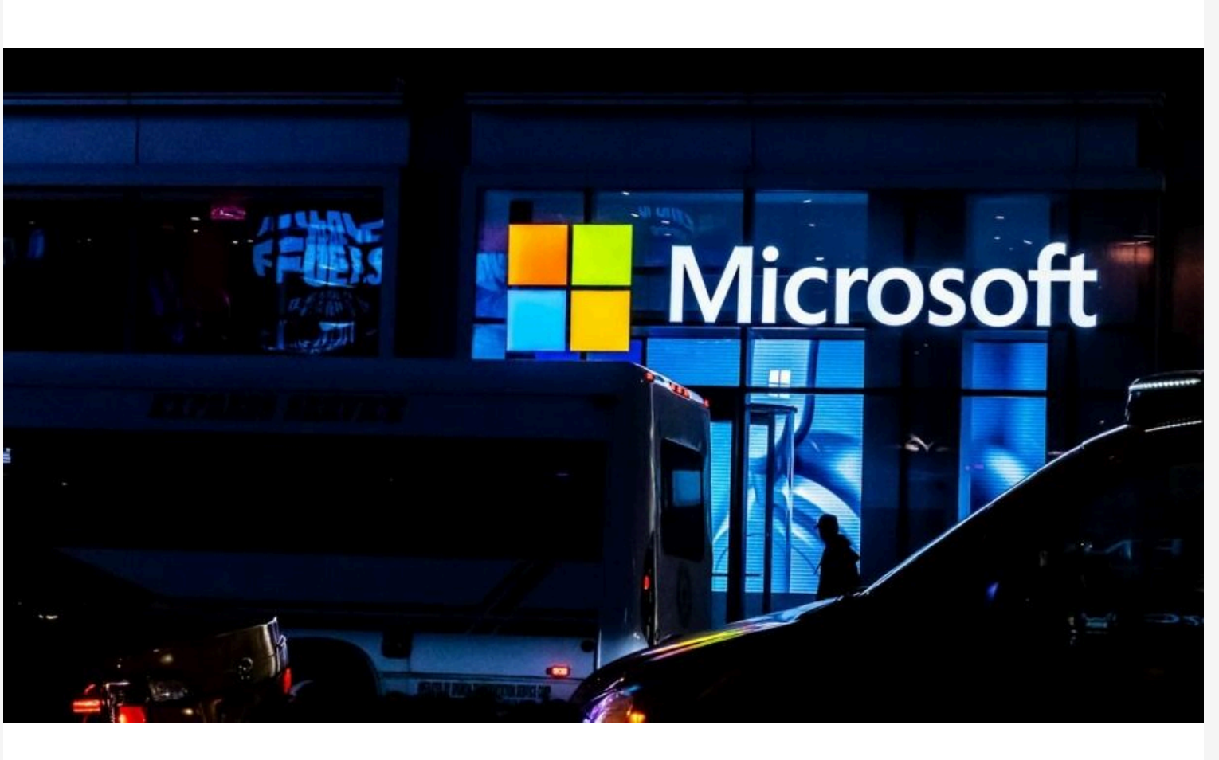

Image credit: Getty Images

9 June 2026

Microsoft addressed 206 vulnerabilities in its latest Patch Tuesday update, marking its largest monthly batch of security patches.

Why it matters: The surge in vulnerabilities highlights an ongoing trend in the tech industry, raising concerns about software reliability.

- Artificial intelligence is increasingly used to discover and patch these vulnerabilities.
- Experts question if this high volume of patches will become the new norm.

The big picture: Half of Microsoft's Patch Tuesday updates this year contained triple-digit flaw counts.

- This year's CVEs surpass the total from 2018.

What's next: Microsoft disclosed three vulnerabilities that were known but not exploited and released an out-of-band patch for an actively exploited zero-day vulnerability.

- The full list of vulnerabilities is available in the Microsoft Security Response Center.

Read full article here

Handala claims Israeli radar hack, but it was only an office phone system

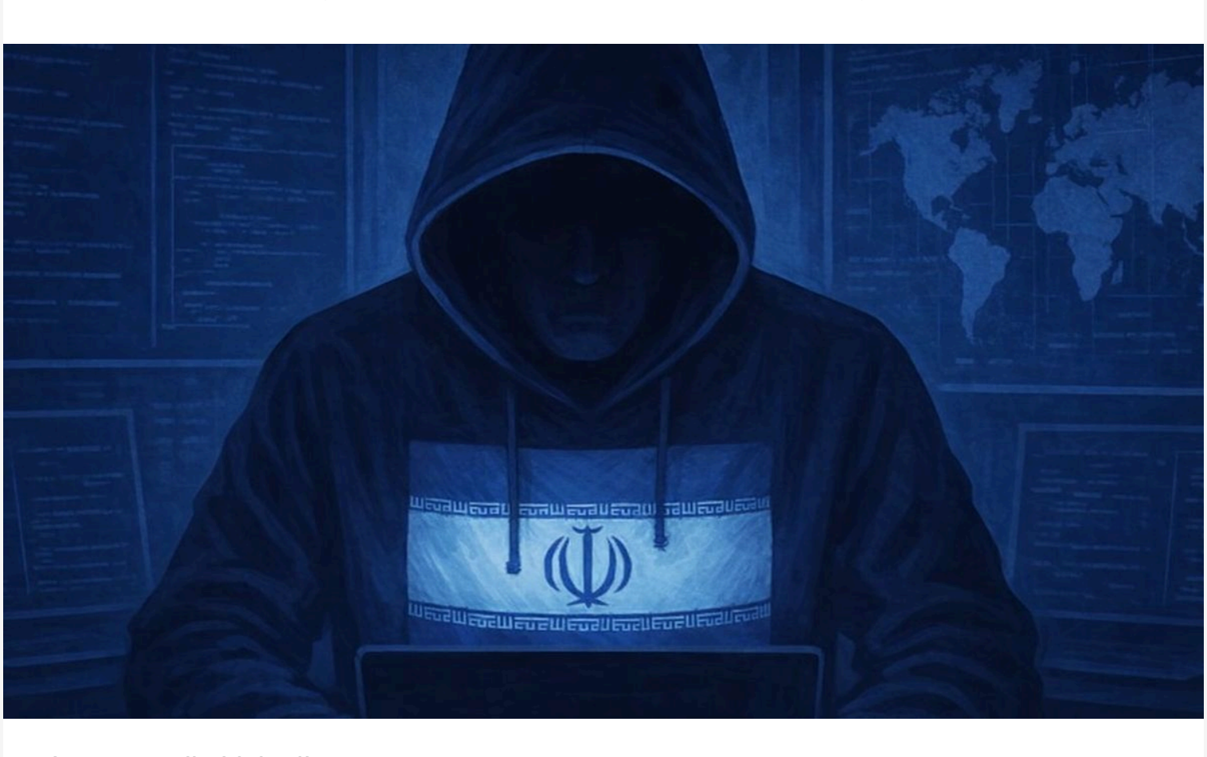

Image credit: LinkedIn

9 June 2026

An Iranian-linked hacker group, Handala, claimed to have disrupted Israeli military radar systems, coinciding with renewed Israel-Iran hostilities on Sunday.

Why it matters: The timing of Handala's claim amidst real-world military tensions raises concerns about psychological warfare tactics.

- The group's threats could influence public perception and international relations.
- Understanding the reality behind these claims is crucial for cybersecurity and geopolitical strategies.

Verifying the claims: Research by SOCRadar debunked Handala's assertions, revealing screenshots of an office phone system panel rather than military infrastructure.

- These findings highlight the importance of verifying claims before reacting, as misinformation can lead to unnecessary escalation.

Handala's history: The group is known for strategically timing claims with real-world events to maximize impact.

- Past operations include breaches of significant entities, emphasizing their ongoing threat.
- Vigilance and skepticism are essential in navigating the complex landscape of cyber warfare.

PT ISAC Analyst Comment: This is the latest example of a hacktivist group overstating their capabilities and impact. In some cases, the false claims become amplified by the media, which may appear to give it additional credibility. It is important to be skeptical of hacktivist claims until verified by authoritative sources.

Read full article here

FROST attack exposes SSD timing vulnerability

Image credit: Bleeping Computer

9 June 2026

A new vulnerability called FROST allows malicious websites to track your online activity via SSD timing.

Why it matters: This attack requires no native code or permissions, turning a local threat into a remote one.

- Websites can exploit the Origin Private File System to monitor SSD activity, bypassing typical security prompts.
- The attack's high accuracy in identifying sites and apps poses significant privacy concerns.

How it works: FROST uses a file larger than your RAM to trigger SSD reads, which are timed to infer your actions.

- The attack sharpens timer resolution by enabling cross-origin isolation on its own page.
- A trained neural network analyzes the timing shifts to identify the sites and apps you use.

What you can do: Current defenses are thin as browser makers consider solutions.

- Google, Mozilla, and Apple have been notified, but responses vary in urgency.
- Closing the attacker's tab stops the measurement, and monitoring storage for large files can help.

The bottom line: The debate continues on whether this level of web app access is a feature or a vulnerability.

Read full article here

Cisco customers encounter another SD-WAN zero-day under attack

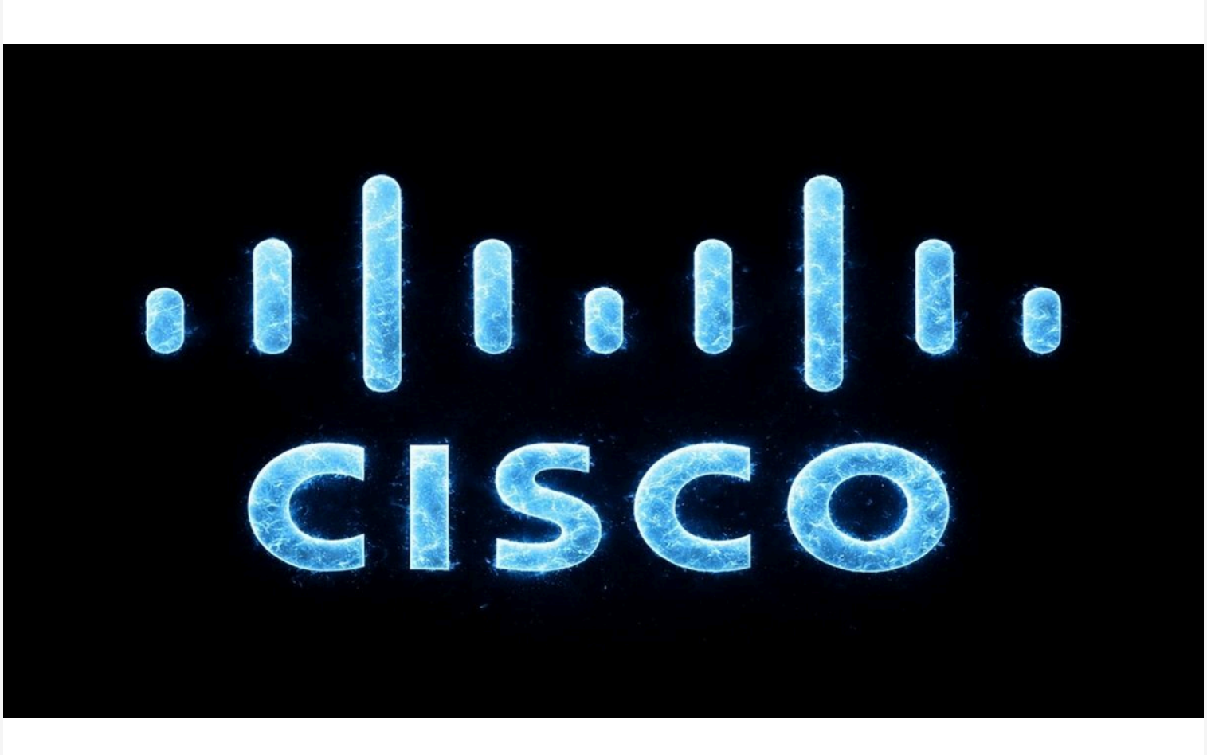

Image credit: Cisco

9 June 2026

Cisco customers are dealing with a newly discovered zero-day vulnerability in the company's SD-WAN management software, adding to a series of security challenges this year.

Why it matters: This vulnerability, identified as CVE-2026-20245, underscores the persistent threat landscape for organizations relying on Cisco's solutions.

- With no current patch or workaround, companies may face increased security risks while awaiting a fix.
- The attack requires valid credentials, potentially limiting its reach but still posing a significant threat to those affected.

The latest: Cisco detected active exploitation earlier this month and disclosed the vulnerability, originally found by Mandiant, without attributing it to any specific group.

- The defect allows attackers with certain access levels to execute command-injection attacks on affected systems.

What's next: Cisco advises upgrading to fixed software released in May for some protection and recommends monitoring for indicators of compromise.

- The company continues to work on a patch and provides guidance for distinguishing between legitimate and malicious activities.

Go deeper: Cisco is one of several security vendors facing a surge in attacks, with seven vulnerabilities affecting its SD-WANs added to the known exploited vulnerabilities catalog this year.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

Microsoft Exchange Flaw Lets Attackers Spoof Any Email Address

US says major Chinese tech giants like Alibaba are supporting China's military

French govt messaging service breached in account hijacking attack

Hackers hijack Microsoft packages to steal developer logins

ServiceNow discloses security incident exposing customer data

GitHub disables Microsoft repos pushing password-stealing malware

Critical Vulnerabilities

Adobe Patches 123 Vulnerabilities

Microsoft Defender 'RoguePlanet' zero-day grants SYSTEM privileges

OpenClaw AI agent found falling for phishing attacks, spills user data

Windows 11 KB5094126 & KB5093998 cumulative updates released

Google patches new Chrome zero-day flaw exploited in the wild

New Veeam vulnerability exposes backup servers to RCE attacks

Mitigation

Proposed Bill Would Restore Funding for MS-ISAC Cyber Program

CISA rethinking how it prioritizes risks, vulnerabilities for feds, private sector

CISA Announces Winners of the 2026 President's Cup Cybersecurity Competition

NCSWIC releases additional content in its Video Series

Cyber Studies

Anthropic's new Fable 5 model is Mythos on a leash

Why OT security remediation stalls after assessment

AI Coding Adoption Hits 97% but Governance Lags Behind

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.