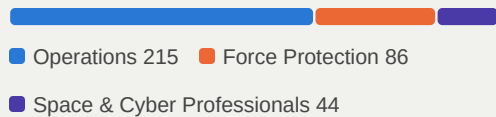


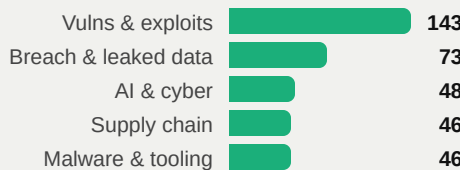
Cyber Watch

BLUF — Edge devices drove the week: Citrix NetScaler intrusions began three weeks before the patch, and Cisco SD-WAN Manager and FortiMail joined KEV. Needs attention: the DMDC breach exposed SSNs and service records of 2.76 million people.

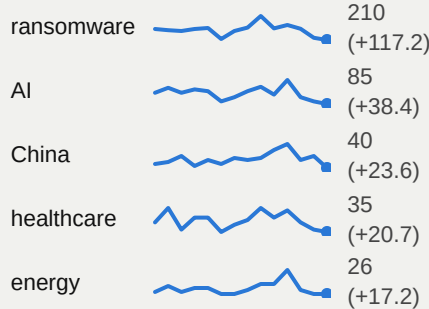
LAST 7 DAYS BY LANE · 345 ITEMS



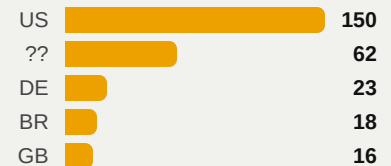
CATEGORIES



RISING TERMS · 7D VS PRIOR



LEAK-SITE VICTIMS BY COUNTRY · 30D



BY THE NUMBERS

Known Exploited Vulnerabilities (KEV) added 4 (0 ransomware-linked) · leak-site victims 184 (90 PACOM AOR)

THREAT ACTOR SPOTLIGHT — UAT-11587 · China-nexus (per Cisco Talos) · Overlaps Jewelbug (Symantec)

WHY NOW

Cisco Talos named UAT-11587 on 30 Sep after ten months of espionage in Asia.

MENTIONS, 30D



PACOM RELEVANCE

Victims include Philippine and Taiwanese government and defense organizations.

NOTABLE TTPS

- Tailored spear-phishing decoys
- Five-stage chain staged on Cloudflare
- Rust backdoor Antino with Outlook/OneDrive C2

COUNTERMEASURES

- Alert on Graph and OneDrive calls from non-browser processes
- Block HTA execution on endpoints
- Share Talos indicators with partner liaisons

Operations

Threats to networks, missions, and infrastructure the command depends on: exploited vulns, intrusions, APT campaigns, ICS/OT, SATCOM/PNT, telecom.

Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway

CISA Cybersecurity Advisories · 2026-09-27

Citrix patched NetScaler zero-days CVE-2026-88771 and -88772 (in KEV) on 27 Sep. According to Mandiant, exploitation began 3 Sep and hit dozens of government, finance and telecom organizations.

So what: NetScaler fronts partner remote access; intrusions predate the patch.

Consider: Recommend checking NetScaler for compromise, not only patch status.

CYBERCOM Vulns & exploits

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Cybersecurity Advisories · 2026-09-30

CISA added Cisco SD-WAN Manager CVE-2026-76504 (auth bypass to admin) and FortiMail CVE-2026-104286 (unauthenticated file write) to KEV on 30 Sep; both were zero-days.

So what: Both sit at the edge of partner networks.

Consider: Consider confirming with the S6 that neither is internet-exposed.

NORTHCOM Vulns & exploits

Force Protection

What Guardians, Airmen, civilians, and families need to know personally: scams, social engineering, apps and devices, OPSEC, breaches of consumer services, official guidance.

Pentagon breach exposes Social Security numbers and military records of millions

Malwarebytes Labs · 2026-10-01

DMDC is notifying about 2.76 million people that attackers took SSNs, birth dates and service details from an unencrypted server, Oct 2025 to Jul 2026 (Malwarebytes, citing CNN). DOW offers 12 months of IDX monitoring.

So what: Guardians and families may be affected; the data aids targeted phishing.

Consider: Consider a commander's call note: IDX, credit freeze, IRS IP PIN.

(NORTHCOM) (Breach & leaked data) (OPSEC & personal security)

China-linked hackers posed as former US officials, Anthropic employee to target AI experts

Nextgov/FCW — cybersecurity · 2026-09-30

According to Proofpoint, China-aligned TA419 posed as a former OSTP official, a former State economist and an Anthropic employee, inviting AI policy experts to a fake advisory committee and then phishing their Microsoft logins.

So what: Staff who work with think tanks get the same invitations.

Consider: Be aware that known names can be spoofed; verify out of band.

(PACOM) (NORTHCOM) (Social engineering) (Cloud & identity) (TA419)

KEY: CVE-2026-86950 — Apple Multiple Products

CISA Known Exploited Vulnerabilities · 2026-09-28

CISA added Apple CoreGraphics CVE-2026-86950 to KEV on 28 Sep. Malwarebytes found a fake iPhone Duo preorder page that runs the DarkSword exploit chain on unpatched iPhones when opened.

So what: Opening one link is enough on an unpatched personal iPhone.

Consider: Recommend updating Apple devices; real preorders open 16 Oct.

(NORTHCOM) (Apps & devices) (Vulns & exploits)

Space & Cyber Professionals

Context for the cyber and space workforce: strategy, doctrine, policy, organization, workforce, standards, exercises, industry and technology trends.

The Pentagon's new cyber mastery incentive model promised a 'new era.' Troops are bracing for pay cuts.

DefenseScoop · 2026-10-01

Cyber Mastery Incentive Pay, part of CYBERCOM 2.0, launched 1 Oct. Documents reviewed by DefenseScoop show cuts of \$100 to \$1,000 a month in at least one branch.

So what: Pay changes bear on retaining cyber operators.

Consider: Recommend reviewing how C-MIP applies to USSF cyber billets.

(CYBERCOM) (Workforce & training) (Strategy & organization)

After reports on suicide deaths, Pentagon puts Cyber Command on notice

The Record (Recorded Future) · 2026-09-30

A 31 Aug memo from the assistant secretary for cyber policy, obtained by Recorded Future News, set demands for CYBERCOM leadership after a cluster of suicide deaths.

So what: Cyber force wellness is now an OSD oversight issue.

Consider: Consider checking in on the welfare of cyber teams.

(CYBERCOM) (Workforce & training) (Strategy & organization)

WATCH LIST

- KEV due 5 Oct: chained Zammad CVE-2026-102489 and -102490.
- SDA PWSA transport launch from Vandenberg, 5 Oct.
- Further Mandiant reporting on NetScaler attribution.
- Fake iPhone Duo preorder lures before 16 Oct.

RECOMMENDATIONS (FOR AWARENESS)

- Recommend checking NetScaler for compromise, not only patch status.
- Consider verifying SD-WAN Manager and FortiMail exposure with the S6.
- Consider a commander's call note on the DMDC breach and Apple updates.