WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Friday, 30 October 2026 | Vol. 2026-303 | As of 300730 EDT OCT 26

BLUF. The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS (=)**. Cisco confirmed in-the-wild exploitation of a firewall VPN flaw that lets an unauthenticated attacker crash ASA and FTD devices, and CISA added it to KEV on 29 Oct; the KEV week now stands at 8 additions, two short of the ABNORMAL band. UNM Health reports a return to normal operations, but University Hospitals' websites and MyChart remain offline a week on. Lithuanian prosecutors confirmed the two Vilnius Starlink suspects are held in Germany on Bulgarian European arrest warrants; no new attack was found. Chips and AI governance stay at **NO CRISIS**. No prediction resolves today; TEC-18 is new.

0. WIRE Technology & Cyber Dashboard

TOPIC	CRISIS LEVEL	DOM. INDICATOR	KEY DRIVER (today)	TREND
TEC-T1 Critical-infrastructure cyber	**ENVIRONMENT FOR CRISIS**	**SIGNIFICANT**	K-3: University Hospitals still offline; Cisco ASA/FTD zero-day in KEV	**=**
TEC-T3 Space and undersea infrastructure	**ENVIRONMENT FOR CRISIS**	**SIGNIFICANT**	O-1: two Starlink attacks in 30 days; suspects held in Germany	**=**
TEC-T4 AI governance and incidents	**NO CRISIS**	**ABNORMAL**	AI-1: AI Act replies under assessment; no proceeding	**=**
TEC-T2 Semiconductors and compute	**NO CRISIS**	**ABNORMAL**	X-1: MOFCOM No. 48 comment period; No. 70 end date 10 Nov unamended	**=**

Indicator: ROUTINE | ABNORMAL | SIGNIFICANT | EXTREME **Crisis level:** NO CRISIS | ENV. FOR CRISIS | POTENTIAL | PROBABLE | IMMINENT

Family level = highest topic level (TEC-T1 and TEC-T3). Roll-up per WIRE_METHOD §1a. Trend key: ↑ toward crisis, ↓ away, = no net change.

Change line. No level changes. TEC-T1 trend ↑ → = (UNM recovery offsets the new Cisco zero-day); TEC-T3 trend ↑ → = (no new attack). Family trend ↑ → =.

Moved indicators (vs 29 Oct). None changed score. K-1 rose from 6 to 8 KEV additions this week, still ROUTINE.

I. TEC-T1 CRITICAL-INFRASTRUCTURE CYBER | ENVIRONMENT FOR CRISIS

Facts. CISA added Cisco Secure Firewall ASA/FTD CVE-2026-76418 and GitLab CVE-2026-97229 to KEV on 29 Oct "based on evidence of active exploitation" (CISA alert, 29 Oct); both carry a 1 Nov due date (KEV JSON). Cisco says an unauthenticated attacker can force a reload of the Remote Access SSL VPN service when secondary authentication is configured, and that its PSIRT "became aware of active exploitation" in October 2026; no actor or victims were named (BleepingComputer; SecurityWeek). NHS England's CSOC assesses further exploitation as "highly likely" (NHS Digital CC-4883). KEV catalogVersion 2026.10.29 has 1,764 entries, 8 added since 26 Oct (KEV JSON); the directives page lists no new emergency directive (CISA directives). CISA's PHP alert was last revised 26 Oct and still does not state observed successful exploitation (CISA PHP alert). PHP has not shipped a fix for CVE-2026-115560 (php.net). UNM says hospitals, clinics and ambulance operations have returned to normal; whether data was taken still awaits FBI forensics (The Record; UNM HSC). University Hospitals says MyChart "remain[s] offline" with no timeline (UH); a spokesperson said disruptions "may continue for the foreseeable future" (Ideastream, 29 Oct). A proposed class action filed 28 Oct alleges patient data theft; UH has not confirmed any (Becker's). Revolve Group disclosed unauthorized access exposing some saved payment cards under 8-K Item 8.01, not 1.05, with no operational disruption (SEC 8-K). Ransomware.live: 136 victims 26–29 Oct vs an 8-week mean of 230/week (feed). **Indicators.** K-1: ROUTINE (8). K-2: ABNORMAL (AA26-281A, carried). K-3: SIGNIFICANT (UH). K-4: ROUTINE (pace about 238/week). K-5: ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** Two edge-firewall stories in one week (PHP2Shell on PAN-OS management planes, a Cisco VPN crash bug) keep TEC-07 live, but a denial-of-service flaw with no named actor is less likely to draw an emergency directive than a code-execution chain. Two more KEV adds by Sunday would push K-1 to ABNORMAL and resolve TEC-03.

II. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | ENVIRONMENT FOR CRISIS

Facts. The Prosecutor General's Office says the two dual-national suspects in the 18 Oct Vilnius attack were named suspects on 27 Oct for forming and taking part in an organised terrorist group, travel for terrorist purposes and a terrorist act, and are detained in Germany under European arrest warrants issued by Bulgaria for a similar offence (Lithuanian Prosecutor's Office, 29 Oct). The lead prosecutor said transfer to Lithuania "will not be resolved in the immediate future" (Delfi EN). No new ground-station or cable attack was found; a 28 Oct quake near Asahi, Japan, caused latency anomalies but no confirmed cable damage (GeoCables). Estonian GNSS-interference warnings remain in force (EANS). **Indicators.** O-1: SIGNIFICANT (2 in 30 days). O-2: ABNORMAL (Baltic GNSS warnings). O-3: ABNORMAL (Cosmos 2612, carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** Bulgaria's warrant takes priority, so any surrender from Germany will most likely go to Sofia first; TEC-17 counts that. The network is being rolled up, which lowers the near-term odds of a repeat by the same cell but says nothing about its sponsor.

III. TEC-T4 AI GOVERNANCE AND INCIDENTS | NO CRISIS

Facts. No new Commission AI Act decision, finding or penalty was found after the 28 Oct statement on information-request replies (2eu.brussels, 28 Oct). No AWS, Azure or Google Cloud post-incident report for 29 Oct was found. **Indicators.** AI-1/2/3: ABNORMAL. **Override −1 to NO CRISIS (held):** no AI incident has disrupted a critical service and no formal proceeding is open.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. MOFCOM Announcement No. 70 (2025) still suspends the October 2025 rare-earth package only "until November 10, 2026" (MOFCOM No. 70 text via Heyuan Magnetics); MOFCOM's 9 Apr briefing tied the suspension to that date (MOFCOM export-control site). No amending notice was found. No new BIS chip rule was found (Federal Register BIS index). **Indicators.** X-1: ABNORMAL (No. 48). X-2 to X-4: ROUTINE. Roll-up: NO CRISIS (=).

V. PREDICTIONS

Resolved: none due. TEC-03 at 8 this week (needs 10). TEC-08 on pace to miss (136 in four days vs about 288 needed). TEC-05/11 open (CISA alert unchanged). TEC-06/12/13 open (UH still "cybersecurity incident", MyChart offline). TEC-14 awaits FBI forensics; TEC-15 still claim-only; TEC-17 open (suspects held in Germany). New (logged in the prediction ledger): - **TEC-18:** Cisco's advisory, CISA or another national cyber agency states that CVE-2026-76418 exploitation achieved more than denial of service (code execution, credential theft or persistence), by 30 Nov 2026. **15%, highly unlikely to unlikely.**

VI. GAPS AND UNVERIFIED

- **Cisco's advisory** (cisco-sa-asaftd-tunnel-dos-s6mgkb75) was read via trade press and NHS Digital, not fetched directly.
- **Third-party outage trackers** reported AWS and Azure incidents on 29 Oct; provider status pages were not confirmed, so these are not scored.
- **Lithuania's Vilnius FIR GNSS warning of 29 Oct** was seen only in a search summary.
- **Leak-site claims** (Qilin on Delta Electric Power Association; a new claim against a US telecom) are unconfirmed.
- **TSMC IR, gpsjam.org, AIID** not queried today; TSMC's October revenue is due about 10 Nov.

Sources

CISA (alerts, KEV, directives); BleepingComputer; SecurityWeek; NHS England Digital; php.net; The Record; UNM HSC; University Hospitals; Ideastream; Becker's Hospital Review; SEC EDGAR; ransomware.live; Lithuanian Prosecutor's Office; Delfi; GeoCables; EANS; 2eu.brussels; MOFCOM; Heyuan Magnetics; Federal Register.