WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Thursday, 12 November 2026 | Vol. 2026-316 | As of 120715 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend **=**, set by critical-infrastructure cyber. CISA added no new exploited flaws on 11 Nov, so the 9–15 Nov KEV count stays at **10**. Ransomware leak sites are running hot: ransomware.live lists **283** victims discovered 9–12 Nov (UTC, 12 Nov partial), against an 8-week mean of about 250 a week. That includes about 50 posted by INC Ransom early on 12 Nov, among them a German municipal water utility that had already confirmed an attack, and three US local governments. Monadnock Community Hospital in New Hampshire has diverted ambulances since about 9 Nov because of a server outage it has not explained (new TEC-39). Vanderbilt still says it does not know what data was taken (new TEC-40). OpenAI logged a nine-hour critical outage of one agent feature. No TEC calls resolve today.

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: EFS cold-room attack still in window; K-4: 283 leak-site victims in under 4 days	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-1: one failed attempt (Lithuania, 18 Oct) in window; no new attributed attack	=
TEC-T4 AI governance and incidents	NO CRISIS	ABNORMAL	AI-3: OpenAI critical incident, ~9.7 h; no new US AI rule	=
TEC-T2 Semiconductors and compute	NO CRISIS	ROUTINE	X-1: no new BIS rule; MOFCOM No. 72 pause still ends 27 Nov	=

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

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

Change line. Family level unchanged at ENVIRONMENT FOR CRISIS; trend moves from ↑ to = because no indicator changed score overnight.

Moved indicators (vs 11 November). None. K-4 stays ROUTINE only because the week has not closed; it is very likely to finish ABNORMAL (above ~313).

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

Facts. The KEV feed is still at catalogVersion **2026.11.10** with **1,779** entries; the 9–15 Nov count is **10** (4 on 9 Nov, 6 on 10 Nov) (KEV feed). CISA's advisories page shows no new alert or advisory after 10 Nov, and the latest Emergency Directive is still ED 26-03 (CISA advisories; CISA directives). The two Barracuda entries fall due tomorrow, 13 Nov (KEV feed). Ransomware.live counts by discovery day are 100 (9 Nov), 67 (10 Nov), 36 (11 Nov) and 80 (12 Nov, through about 10:20 UTC) (feed). Of the 12 Nov entries, about 50 are INC Ransom posts made within 16 minutes. They include Stadtwerke Waldbröl GmbH, plus the City of Princeton, Somervell County and Beaver County PA (same feed). Stadtwerke Waldbröl, which runs drinking water, wastewater and street lighting, says on its homepage that attackers encrypted parts of its IT and may have stolen customer data. It says supply was not affected (Stadtwerke Waldbröl). Local paper Oberberg-Aktuell reported the notice on 30 Oct and said state police (LKA) are investigating (Oberberg-Aktuell). Ridgecrest Regional Hospital (California) confirmed a 9 Nov cyber incident that took down its phones and computers. Clinics have reopened, and its lab draw station reopened on 11 Nov (Ridgecrest Daily Independent; Becker's). Monadnock Community Hospital (New Hampshire, 25 beds) is diverting ambulances and has postponed major elective surgery because of a server outage. It says it is working with outside experts but has not said whether the outage is cyber-related (DysruptionHub). Vanderbilt's 1 p.m. 11 Nov update says it is working with government agencies and law enforcement. Its FAQ still says it is "determining what, if any, data may have been accessed" (Vanderbilt updates; Vanderbilt FAQ). EDGAR full-text search shows no 8-K Item 1.05 filing dated 1–12 Nov (EDGAR FTS). **Indicators.** K-1 ABNORMAL (10 of 9–15 Nov); K-2 ABNORMAL (carried; Barracuda forensic-triage deadline 13 Nov); K-3 SIGNIFICANT (EFS, 2 Nov, in window; Ridgecrest and Waldbröl are single sites with services restored or unaffected, not a utility or hospital chain); K-4 ROUTINE (week open; 283 in 4 partial days); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** The leak-site jump comes mostly from one gang dumping a backlog, and the Waldbröl attack dates from October, so the count overstates new activity this week. Even so, the 9–15 Nov total will almost certainly exceed 299, so TEC-32 (180–299, resolves 16

Nov) is now very unlikely to hit. US hospital outages that start without explanation, as at Monadnock, have often been confirmed as cyber incidents within days (TEC-39).

II. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | NO CRISIS

Facts. No new attributed ground-station or cable attack found for 11–12 Nov. Vocus completed the repair of the Australia Singapore Cable on 11 Nov after a fault in Indonesian waters on 4 Sep. Its notice records a "suspected shunt fault", not sabotage (00Shark, quoting the Vocus notice). Taiwan's Maritime Port Bureau has scheduled repairs of the EAC1 cable off eastern Taiwan for 10 Nov–20 Dec (SubTel Forum). **Indicators.** O-1 ABNORMAL (1 failed attempt in 30 days); O-2 ABNORMAL (carried); O-3 ABNORMAL (carried). **Override −1 to NO CRISIS (held):** the only event in the window failed, and no attack has been confirmed in 25 days. Trend =. **Analyst Comment.** Repairs are closing out earlier faults with no attribution, so this topic's risk still rests on the Gulf of Oman cable corridors described in yesterday's edition.

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

Facts. OpenAI's status page logged a **critical** incident, "Unable to start new Workspace Agent runs", from 22:50 UTC on 11 Nov to 08:32 UTC on 12 Nov (about 9.7 hours), plus a 9-minute login and sign-up error spike earlier on 11 Nov (OpenAI status). AWS reports a resolved EC2 API and launch issue in Tokyo (AWS Health). The Federal Register shows no document mentioning "artificial intelligence" published since 11 Nov (FR API). **Indicators.** AI-1/2/3 ABNORMAL. **Override −1 to NO CRISIS (held):** the outages hit single products or regions, not critical services, and there is no formal AI Act finding.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. No BIS document published since 10 Nov (FR API). No MOFCOM announcement extending the No. 72 (2025) pause was found; that pause ends 27 Nov (MOFCOM). **Indicators.** X-1 ROUTINE; X-2–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =.

V. PREDICTIONS

Resolved: none. **Due soon:** TEC-10 (PHP fix for CVE-2026-115560 by 13 Nov; php.net still shows no release after 21 Oct, and the 3 Nov release candidates do not confirm a fix), TEC-32 (now very unlikely to hit) and TEC-33 (count already at 10), both on 16 Nov. **Open:** TEC-01, 05–07, 09, 10, 12, 14–19, 21–25, 27–29, 31–38. **New:** - **TEC-39:** Monadnock Community Hospital or a US authority confirms that its November outage was a cyberattack or cybersecurity incident by 30 Nov 2026. **55%, about even.** - **TEC-40:** Vanderbilt confirms that personal data was accessed or taken in its 9 Nov incident by 15 Dec 2026. **60%, likely.**

VI. GAPS AND UNVERIFIED

- The INC Ransom listings of three US local governments are leak-site claims only, and none was checked for a confirmation today.
- The NEA (Climax Inc) and Methodist Hospitals (Osiris) claims are still unconfirmed by either organisation.
- Monadnock's outage cause is unconfirmed. Regional dispatchers' account of when diversion began is second-hand.
- Ransomware.live counts use UTC discovery dates and are often backfilled. gpsjam not refreshed today (O-2 carried). AIID not rechecked.

Sources

CISA KEV, advisories and directives; ransomware.live; Stadtwerke Waldbröl; Oberberg-Aktuell; Ridgecrest Daily Independent; Becker's Hospital Review; DysruptionHub; Vanderbilt News; SEC EDGAR; 00Shark (Vocus notice); SubTel Forum; OpenAI status; AWS Health; Federal Register; MOFCOM.