WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Wednesday, 11 November 2026 | Vol. 2026-315 | As of 110720 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend ↑, set by critical-infrastructure cyber. On 10 Nov CISA added **6** more actively exploited flaws to its KEV catalog, bringing the 9–15 Nov week to **10** in two days, so K-1 moves to ABNORMAL. Two of them are a Barracuda email-gateway chain that gives root access, with a 3-day federal deadline of 13 Nov. Another is an Outlook zero-day fixed on Patch Tuesday that leaks NTLM password hashes. Ransomware leak sites listed **181** victims on 9–11 Nov, against an 8-week mean of about 250 a week. One new group claims Nepal's state power utility, but the utility has not confirmed an incident. Vanderbilt still calls its incident a "hacking incident" and warns that full restoration may take weeks (TEC-36 open). No TEC calls fall due today. TEC-37 and TEC-38 are 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-1: 10 KEV adds 9–10 Nov (Barracuda chain, Outlook zero-day); K-3: EFS cold-room attack still in window	↑
TEC-T3 Space and undersea infrastructure	**NO CRISIS**	**ABNORMAL**	O-1: one failed attempt (Lithuania, 18 Oct) in window; Iran-linked ships loitering over Gulf of Oman cables	=
TEC-T4 AI governance and incidents	**NO CRISIS**	**ABNORMAL**	AI-1: EU AI Office request to OpenAI and Anthropic still open; no new US AI rule	=
TEC-T2 Semiconductors and compute	**NO CRISIS**	**ROUTINE**	X-1: no new BIS rule; MOFCOM No. 72 pause clock runs to 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 K-1 rises. No topic changes level.

Moved indicators (vs 10 November). K-1 ROUTINE → ABNORMAL (10 adds so far in 9–15 Nov; the band is 10–20). K-4 stays ROUTINE because the week has not closed, but it is running hot. No other moves.

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

Facts. KEV catalogVersion **2026.11.10** lists **1,779** entries. On 10 Nov CISA added CVE-2026-20320 (Cisco BroadWorks), CVE-2026-111560 and CVE-2026-116606 (Barracuda), CVE-2026-111793 (Openwave Webtop), CVE-2026-124194 (Microsoft Outlook) and CVE-2026-125350 (Chromium) (CISA alert; KEV feed). The two Barracuda entries are due 13 Nov, require forensic triage under BOD 26-04, and can be chained (KEV catalog). The other four are due 24 Nov (KEV feed). Barracuda says the chain can give root on its email gateway and that it has seen exploitation "affecting a small number of organizations" (advisory update of 9 Nov) (Barracuda). Microsoft's November updates fix an Outlook flaw, exploited in the wild, that sends a user's NTLMv2 hash to an attacker-controlled server when a crafted message file is opened (JPCERT/CC; BleepingComputer). The latest Emergency Directive is still ED 26-03 (CISA). On ransomware.live, **181** victims were discovered on 9–11 Nov (UTC; 11 Nov partial). Among them is Nepal Electricity Authority, claimed on 10 Nov by "Climax Inc", which the site flags as an emerging group, and Methodist Hospitals in Northwest Indiana, claimed by Osiris on 11 Nov (feed; NEA entry). EDGAR full-text search shows no 8-K Item 1.05 filing since 13 Oct (EDGAR FTS). Vanderbilt's 6 p.m. 10 Nov update says it is still containing the incident and that full restoration "may take multiple weeks". It does not use the word ransomware (Vanderbilt). **Indicators.** K-1 ABNORMAL (10 of 9–15 Nov); K-2 ABNORMAL (three-day deadlines, Outlook zero-day); K-3 SIGNIFICANT (EFS, 2 Nov, in window; no new confirmed utility, pipeline or hospital-chain disruption); K-4 ROUTINE (week not closed; 181 in 3 days against a weekly mean of ~250); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** This is the second straight batch of three-day deadlines, which is likely to push the weekly KEV count past 10 well before Sunday. TEC-33 is already met on the count and resolves on 16 Nov. At the current pace, ransomware.live will very likely exceed 299 victims for 9–15 Nov, so TEC-32 (180–299) now looks unlikely to hit. The Nepal utility and Methodist Hospitals listings are claims only and do not move K-3 unless they are confirmed (see TEC-37 and TEC-38).

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

Facts. No new attributed ground-station or cable attack found for 10–11 Nov. Ars Technica reports, citing the Financial Times and Windward, that three sanctioned Iran-linked tankers and an Iranian fishing boat loitered over subsea cable corridors in the Gulf of Oman in October, some with AIS switched off. It also quotes an IRGC spokesperson on 20 Oct reminding "the enemy" of the cables (Ars Technica). **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 24 days. Trend =. **Analyst Comment.** Loitering is a warning sign, not an attack. A Gulf cable cut would very likely raise this topic at once because four Gulf states rely entirely on subsea links through Hormuz (Ars Technica, same link).

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

Facts. The Federal Register shows no document mentioning "artificial intelligence" published since 10 Nov (FR API). The EU AI Office's 6 Nov request to OpenAI and Anthropic about AI-agent incidents remains a request for information (Rapporteur). **Indicators.** AI-1/2/3 ABNORMAL. **Override −1 to NO CRISIS (held):** no critical-service AI disruption and no formal AI Act finding.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. No new BIS rule since FR 2026-22793 on 9 Nov (FR API). MOFCOM/GAC Announcement 2026 No. 58 extends the pause on six 2025 export-control announcements (MOFCOM). It does not cover No. 72 (2025), whose US-specific gallium, germanium and antimony pause ends 27 Nov. **Indicators.** X-1 ROUTINE; X-2–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =. **Analyst Comment.** TEC-09 (No. 72 extension by 27 Nov) remains the main dated risk in this topic.

V. PREDICTIONS

Resolved: none due today. **Due soon:** TEC-10 (PHP fix for CVE-2026-115560 by 13 Nov; php.net news still shows no release after 26 Oct), TEC-32 and TEC-33 (16 Nov; TEC-33 count already at 10). **Open:** TEC-01, 05–07, 09, 10, 12, 14–19, 21–25, 27–29, 31–36. **New:** - **TEC-37:** Nepal Electricity Authority or a Nepal government body confirms a cyber incident at the utility by 30 Nov 2026. **30%, unlikely.** - **TEC-38:** Methodist Hospitals (Northwest Indiana) or a US authority confirms a cybersecurity incident involving the claimed November attack by 15 Dec 2026. **40%, unlikely.**

VI. GAPS AND UNVERIFIED

- The NEA (Climax Inc, "20TB") and Methodist Hospitals (Osiris, "579.22GB") claims are leak-site claims only, and neither organisation has confirmed them.
- BYOD's claim of more than 1 million SSNs from Vanderbilt has not been confirmed by the university.
- Brief OpenAI and Anthropic API incidents on 10 Nov were seen only on third-party trackers.
- gpsjam not refreshed today (O-2 carried). AIID not rechecked. Ransomware.live counts use UTC discovery dates and can be backfilled.

Sources

CISA KEV and alerts; CISA Directives; Barracuda; JPCERT/CC; BleepingComputer; ransomware.live; SEC EDGAR; Vanderbilt News; Ars Technica; Federal Register; Rapporteur; MOFCOM.