WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Tuesday, 10 November 2026 | Vol. 2026-314 | As of 100720 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend **=**, set by critical-infrastructure cyber. On 9 Nov CISA added **4** actively exploited flaws to its KEV catalog, all with a **12 Nov** federal deadline; one is the OpenSSH "SSHole" authentication bypass on musl-based Linux such as Alpine, which several firms saw exploited from 6–7 Nov. Vanderbilt University is containing a ransomware attack that shut its networks on 9 Nov; its hospital says it was not affected. TSMC reported record October revenue of **NT$586.89 billion**, inside the TEC-30 range, so TEC-30 resolves as a hit. Germany arrested a man accused of commissioning the September Starlink ground-station arson in Poland, which is an arrest, not a new attack. The EU AI Office sent OpenAI and Anthropic a second round of questions on AI-agent incidents. TEC-35 and TEC-36 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-3: EFS cold-room attack still in window; K-2: SSHole and 3 other KEV adds, 3-day deadline	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-1: one failed attempt (Lithuania, 18 Oct) in window; third Poland suspect arrested	=
TEC-T4 AI governance and incidents	NO CRISIS	ABNORMAL	AI-1: EU AI Office second request for information on agent incidents	=
TEC-T2 Semiconductors and compute	NO CRISIS	ROUTINE	X-3: TSMC October revenue record, +59.7% y/y	=

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 =. No topic changes level.

Moved indicators (vs 9 November). K-1 stays ROUTINE (4 adds so far for 9–15 Nov). K-2 stays ABNORMAL, with a fresh driver (SSHole). X-3 confirmed ROUTINE with the October print. No other moves.

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

Facts. KEV catalogVersion **2026.11.09** lists **1,773** entries. On 9 Nov CISA added CVE-2026-123158 (OpenSSH), CVE-2026-102895 (GPUStack), CVE-2026-116779 (SignalWire FreeSwitch) and CVE-2026-123218 (IBM Aspera Faspex), each with a due date of 12 Nov and required action citing BOD 26-04 (KEV). SSHole lets an attacker log in to accounts whose password field is "" *by sending a 257–1,024-character password on musl-based Linux without PAM; OpenSSH 10.6p2 fixed it on 5 Nov (SecurityWeek). GreyNoise recorded its first successful exploitation on 7 Nov at 00:46 UTC, and one attacker gained root and installed a command-and-control agent that never reached its server (BleepingComputer). WatchTowr says only botnets and crypto miners are using it so far (SecurityWeek, same link). CISA's directives page still shows no Emergency Directive newer than ED 26-03 (CISA). Vanderbilt University said on 9 Nov it was containing an "active cybersecurity incident"; Vanderbilt Health said its hospital and clinics were not affected, and the BYOD group appears to have claimed it (Nashville Banner). Ransomware.live lists "Vanderbilt EDU" discovered 9 Nov, and counts 100 victims discovered on 9 Nov and 44 so far on 10 Nov (feed). Indicators. K-1 ROUTINE (4 of 9–15 Nov); K-2 ABNORMAL; K-3 SIGNIFICANT (EFS, 2 Nov, in window); K-4 ROUTINE (week not closed); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. Analyst Comment.* The 3-day KEV deadline is far shorter than the 14 days CISA gave the SonicWall entry added on 6 Nov, which suggests that CISA sees urgent federal exposure. SSHole's reach is narrow (Alpine, OpenWrt, Buildroot and many container images) but includes embedded and edge devices, so a confirmed operational compromise is likely to surface in time (see TEC-35). Vanderbilt is a university, not critical infrastructure, so it does not move K-3. A single-day spike of 100 ransomware victims usually reflects a leak-site dump rather than 100 new attacks on that day.

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

Facts. No new attributed ground-station or cable attack found for 9–10 Nov. The Baden-Württemberg criminal police and the Stuttgart prosecutor general said special forces arrested a Turkish citizen in the Reutlingen district, accused of commissioning the September arson at the Starlink station south of Warsaw; eight phones and ammunition were seized (DIE ZEIT). The arrest date is reported as 3 Nov (Spiegel). **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 23 days. Trend =. **Analyst Comment.** The arrest strengthens the case that the Poland, Bulgaria and Lithuania attacks were one commissioned network, which supports TEC-17 but does not add a new event.

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

Facts. A Commission spokesperson said on 9 Nov that the AI Office sent OpenAI and Anthropic new questions on 6 Nov about how many AI-agent incidents occurred, where the EU was affected, and how safety practices changed; reports describe a request for information, not a finding (LLMs Blog, citing Rapporteur, ECO and DN). The Federal Register shows no AI governance rule since 9 Nov (FR API). GitHub logged a 49-minute major incident on 9 Nov degrading two OpenAI models in Copilot (GitHub status). **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. TSMC October 2026 consolidated revenue was about **NT$586.89 billion**, up 14.7% from September and 59.7% from October 2025; January–October totalled NT$4,485.62 billion, +43.3% (TSMC). That beats the prior monthly high of NT$514.81 billion in August (TSMC monthly revenue). No new BIS rule since FR 2026-22793 on 9 Nov (FR API). **Indicators.** X-1 ROUTINE; X-2–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =. **Analyst Comment.** Record output shows no fab or supply disruption. TEC-09 (MOFCOM No. 72, 27 Nov) remains the main dated risk in this topic.

V. PREDICTIONS

Resolved: TEC-30 HIT (October revenue NT$586.89B, inside NT$435.08–588.64B; p 0.85, Brier 0.0225). **Due soon:** TEC-10 (PHP fix for CVE-2026-115560 by 13 Nov; php.net still shows no fixed release), TEC-32 and TEC-33 (weekly counts, 16 Nov). **Open:** TEC-01, 05–07, 09, 10, 12, 14–19, 21–25, 27–29, 31–34. **New:** - **TEC-35:** A national cyber agency or an affected organisation confirms, by 30 Nov 2026, a successful compromise of an organisation's system via SSHole (CVE-2026-123158). **30%, unlikely.** - **TEC-36:** Vanderbilt University, by 30 Nov 2026, uses the word ransomware in an official statement about the 9 Nov incident. **45%, about even.**

VI. GAPS AND UNVERIFIED

- An aggregator digest claims GitHub Copilot was down 24 hours on 9 Nov; GitHub's own status page shows shorter incidents, so WIRE does not use that figure.
- The BYOD claim on Vanderbilt is from leak-site messages; the university has not named ransomware.
- A Financial Times report, citing Windward, that Iran-linked vessels lingered over Gulf of Oman cable routes was seen only second-hand.
- gpsjam not refreshed today (O-2 carried). AIID and EDGAR Item 1.05 not rechecked.

Sources

CISA KEV; CISA Directives; SecurityWeek; BleepingComputer; Nashville Banner; ransomware.live; DIE ZEIT; Spiegel; LLMs Blog; Federal Register; GitHub status; TSMC.