WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Saturday, 31 October 2026 | Vol. 2026-304 | As of 310730 EDT OCT 26

BLUF. The WIRE Technology & Cyber level holds at **ENVIRONMENT FOR CRISIS**, with the trend turning ↑. CISA added two Ivanti Connect Secure flaws to KEV on 30 Oct and says attackers are chaining them with an earlier bug to run commands without authentication and steal credentials and data. That brings the KEV week to 10 additions, moving K-1 to ABNORMAL and resolving TEC-03 as a hit. Ransomware leak-site postings jumped to 75 on 31 Oct alone, putting the week at 253 against a mean of 230. University Hospitals still has MyChart and electronic prescribing down. No new ground-station or cable attack was found, and chips and AI governance stay at **NO CRISIS**. TEC-19 and TEC-20 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: University Hospitals e-prescribing and MyChart down; K-1: Ivanti chain lifts KEV week to 10	↑
TEC-T3 Space and undersea infrastructure	**ENVIRONMENT FOR CRISIS**	**SIGNIFICANT**	O-1: two Starlink attacks in 30 days; police link all three	=
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. 70 end date 10 Nov still 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 = to ↑ (K-1 to ABNORMAL, Ivanti chain confirmed for credential theft, ransomware postings above the mean). Family trend = to ↑.

Moved indicators (vs 30 Oct). K-1 ROUTINE to ABNORMAL (8 to 10 KEV additions in the week of 26 Oct). K-4 still ROUTINE, but the week-to-date count (253) has passed the 8-week mean.

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

Facts. CISA added Ivanti Connect Secure CVE-2026-111357 and CVE-2026-118527 to KEV on 30 Oct "based on evidence of active exploitation" (CISA alert, 30 Oct). KEV gives CVE-2026-111357 a 2 Nov due date with forensic triage required, and catalogVersion 2026.10.30 lists 1,766 entries, 10 added since 26 Oct (KEV JSON). CISA's revised Ivanti alert says threat actors are exploiting CVE-2026-104935, CVE-2026-111357 and CVE-2026-118527 for "remote, unauthenticated execution of arbitrary commands, to conduct credential theft and data exfiltration," and warns that Ivanti's Integrity Checker Tool may miss the in-memory activity (CISA Ivanti alert, revised 30 Oct). Belgium's CCB says Ivanti confirmed the chain gives pre-authentication code execution as root (CCB), and Canada's Cyber Centre updated its advisory the same day (CCCS AV26-1035). Volexity, which found the chain, tracks the actor as UTA0576 and has not attributed it (Volexity). The directives page shows no new emergency directive (CISA directives). PHP still lists no fixed release for CVE-2026-115560 (php.net). A University Hospitals internal letter says electronic prescribing is not working and "we do not have a clear estimate on when all systems will return to normal, including MyChart" (WKYC, 30 Oct); UH declined to say whether ransomware was involved (BankInfoSecurity). Its public page still says "unusual activity" (UH). Ransomware.live counts 253 victims discovered 26–31 Oct, including 75 on 31 Oct, against an 8-week mean of 230 per week (feed). **Indicators.** K-1: ABNORMAL (10). K-2: ABNORMAL (AA26-281A, carried). K-3: SIGNIFICANT (UH). K-4: ROUTINE (week to date 110% of mean). K-5: ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend ↑. **Analyst Comment.** This is the third edge-device chain in a week, after the PHP management-plane bugs and the Cisco VPN crash flaw, and the only one where CISA itself states credential theft and data exfiltration. The 2 Nov due date and forensic-triage flag suggest CISA wants federal hunts done before patching alone, which makes a directive somewhat more likely than yesterday; TEC-07 stays at 25% until one appears. Most of the 31 Oct jump comes from one group posting in bulk, so TEC-08 now looks likely to hit on Monday's check, but that reflects one gang's posting habits more than a broad surge.

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

Facts. Lithuanian police said on 29 Oct that the same two men are suspected in the Lithuanian and Bulgarian Starlink attacks and that the Polish perpetrators were connected to them; both suspects were detained in Duisburg on 23 Oct on Bulgarian warrants (The Insider, 30 Oct; Al Arabiya, 29 Oct). No new ground-station or cable attack was found. **Indicators.** O-1: SIGNIFICANT (2 in 30 days). O-2: ABNORMAL (Baltic GNSS warnings, carried). O-3: ABNORMAL (carried). Roll-up: ENVIRONMENT FOR CRISIS. Trend =.

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

Facts. No Commission AI Act decision, finding or penalty was found after the 28 Oct statement. No major cloud post-incident report for 30 Oct was found; the latest Google Cloud report covers the 20 Oct europe-west2-b power event (Google Cloud status). **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. As of 29 Oct, neither government had published legal text carrying its export-control suspensions past 9–10 Nov (E+E Leader); MOFCOM's 9 Apr briefing tied the No. 70 suspension to 10 Nov 2026 (MOFCOM export-control site). No new BIS chip rule was found (Federal Register BIS index). **Indicators.** X-1: ABNORMAL. X-2 to X-4: ROUTINE. Roll-up: NO CRISIS (=).

V. PREDICTIONS

Resolved: TEC-03 HIT (KEV reached 10 additions in the week of 26 Oct; p 0.65, Brier 0.1225). TEC-08 checks on 2 Nov (253 so far, about 288 needed). TEC-05/11 open (CISA PHP alert unchanged). TEC-06/12/13 open. TEC-02 open, 10 days to the No. 70 end date. New (logged in the prediction ledger): - **TEC-19:** CISA, FBI, NSA or another national cyber agency, or Ivanti, publicly attributes exploitation of the Ivanti Connect Secure chain (CVE-2026-104935, -111357, -118527) to a named state-sponsored or state-linked actor by 30 Nov 2026. **30%, unlikely.** - **TEC-20:** CISA KEV adds 10 or more entries in the week of Mon 2 Nov to Sun 8 Nov 2026. **40%, unlikely to roughly even chance.**

VI. GAPS AND UNVERIFIED

- **Ivanti's own advisory** was read via CISA, CCB and CCCS, not fetched directly; no victim count is public.
- **A Brussels Post report** that the AI Office has begun enforcing AI Act transparency rules was not matched to a Commission release; not scored.
- **Leak-site claims** in the 31 Oct bulk posting (including large technology firms) are unconfirmed and not named here.
- **TSMC IR, gpsjam.org, AIID and EDGAR full-text search** not queried today; TSMC's October revenue is due about 10 Nov.

Sources

CISA (alerts, KEV, directives); CCB Belgium; Canadian Centre for Cyber Security; Volexity; php.net; WKYC; BankInfoSecurity; University Hospitals; ransomware.live; The Insider; Al Arabiya; Google Cloud status; E+E Leader; MOFCOM; Federal Register.