WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Saturday, 14 November 2026 | Vol. 2026-318 | As of 140716 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, and the trend levels off from ↑ to **=** because Microsoft has now declared the Microsoft 365 outage over. Microsoft's status page says services are fully recovered and the email backlog is cleared, and it gives an end time of 11:10 a.m. ET on 13 Nov. Check Point confirms a firewall zero-day (CVE-2026-123039) exploited against about two dozen customers, with ESXi wiping at Israeli organisations; CISA listed it on 13 Nov (week count 12). Ransomware.live now lists **323** victims for 9–14 Nov, above the alert line of 312. **TEC-41 resolved as a hit; TEC-10 resolved as a miss.**

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 in window; K-4: 323 leak-site victims, 9–14 Nov	=
TEC-T4 AI governance and incidents	ENVIRONMENT FOR CRISIS	SIGNIFICANT	AI-3: Microsoft 365 outage (12–13 Nov), now resolved, still in window	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-1: one failed attempt (Lithuania, 18 Oct) in window	=
TEC-T2 Semiconductors and compute	NO CRISIS	ROUTINE	X-1: no new BIS rule; MOFCOM No. 72 pause ends 27 Nov	=

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

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

Change line. The family level stays at ENVIRONMENT FOR CRISIS. The trend moves from ↑ to = because the outage that drove TEC-T4 is over and no topic moved up.

Moved indicators (vs 13 November). K-1 count 10 → 12 (still ABNORMAL). K-4 ROUTINE → **ABNORMAL** (323 against an alert line of about 312).

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

Facts. CISA added two exploited flaws on 13 Nov: UnrealIRCd CVE-2026-114713 and Check Point CVE-2026-123039. The catalog is now at version **2026.11.13** with **1,781** entries, and the 9–15 Nov count is **12** (KEV feed; CISA alert). Check Point reports "an active exploit of this vulnerability against a couple of dozen customers" and has issued hotfixes (sk1000362). Its researchers say attacks began 30 Oct via PHP2Shell on Mobile Access portals. The first wave, against Israeli organisations, ended with the destroy_v6 wiper on VMware ESXi hosts; a broader 2 Nov wave was not destructive. Attribution is low confidence, and a false flag is not ruled out (Check Point Research). No new emergency directive is listed (CISA directives). Ransomware.live daily counts for 9–14 Nov (UTC) are 100, 67, 36, 99, 19 and 2, a total of **323**. The 8-week mean is 249.75 (feed). Monadnock Community Hospital's update at 5:30 p.m. on 13 Nov says it expects to stay on downtime procedures through 18 Nov, has no confirmed date for full restoration, and remains on ambulance diversion (MCH). Vanderbilt (13 Nov) says most systems are back but cloud storage stays disabled during the "ongoing cyberattack" (Vanderbilt updates). An EDGAR full-text search found no 8-K filing citing Item 1.05 for 9–14 Nov (EDGAR FTS). **Indicators.** K-1 ABNORMAL (12); K-2 ABNORMAL (carried); K-3 SIGNIFICANT (EFS, 2 Nov, in window; Monadnock is a single site with no confirmed cyber cause); K-4 **ABNORMAL** (323 > 1.25 × mean); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** The Check Point campaign is the most serious new item. It shows destructive intent against Israeli targets through a perimeter device that many networks rely on. It does not meet the K-3 bar yet: no named utility, pipeline or hospital has confirmed a disruption. The week will very likely close above the alert line, so TEC-32 (180–299) will almost certainly miss when it is scored on 16 Nov.

II. TEC-T4 AI GOVERNANCE AND INCIDENTS | ENVIRONMENT FOR CRISIS

Facts. Microsoft's final status update, last updated at 10:51 p.m. ET on 13 Nov, says: "services across the previously affected environments have fully recovered and the backlog of email messages has been processed." It gives an end time of 16:10 UTC (11:10 a.m. ET) on 13 Nov (Microsoft 365 status). Reuters reports that early on 14 Nov Microsoft posted on X that it had "restored service to the remaining impacted customers and regions." Reuters says government agencies on three continents and some trading firms were affected (Reuters via Investing.com). A university status page relays Microsoft's explanation: the incident came from an issue during an earlier network capacity upgrade that surfaced after a recent network change, and it was not related to cyber activity or AI (UQ status). The Federal Register shows no new AI rule; the only match since 13 Nov is a request for information (FR API). **Indicators.** AI-1 ABNORMAL; AI-2 ABNORMAL; AI-3 SIGNIFICANT (the multi-region outage stays in the scoring window even though it is resolved). Roll-up: ENVIRONMENT FOR CRISIS. Trend = (no new incident). **Analyst Comment.** TEC-T4 is likely to step down once the outage leaves the window, unless the post-incident report shows a wider weakness.

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

Facts. No new attributed ground-station or cable attack was found for 13–14 Nov. The UK is preparing laws that would allow jail terms of up to 14 years for deliberately damaging undersea cables and pipelines (Euronews). **Indicators.** O-1/O-2/O-3 ABNORMAL (carried). **Override −1 to NO CRISIS (held):** the only event in the window failed. Trend =.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. No BIS document has been published since 12 Nov (FR API). Under MOFCOM Announcement No. 58 of 2026 (9 Nov), the October 2025 rare-earth controls stay suspended to 10 Jan 2027. The pause on gallium, germanium and antimony curbs still ends 27 Nov (Chemical Week; Washington Examiner). **Indicators.** X-1–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =.

V. PREDICTIONS

Resolved: - **TEC-41** (Microsoft says the outage is resolved by 14 Nov, p 0.70): **hit**, Brier **0.09** (Microsoft 365 status). - **TEC-10** (PHP fix naming CVE-2026-115560 by 13 Nov, p 0.70): **miss**, Brier **0.49**. php.net still lists 8.5.12 (21 Oct) as current, and the newest php-src advisories date from 21 Oct (php.net releases; php-src advisories).

Pending: TEC-33 (KEV ≥ 10, 9–15 Nov) is already at 12 and TEC-32 (180–299 victims) is already above its range. Both are scored on 16 Nov per their criteria. TEC-42 (Monadnock diversion lifted by 18 Nov) is still open.

New: - **TEC-43:** CISA adds 10 or more vulnerabilities to its exploited-vulnerability catalog in the week of 16–22 Nov. **40%, unlikely**. - **TEC-44:** Ransomware.live lists 330 or more victims discovered 16–22 Nov (1.25 × the 8-week mean). **30%, unlikely.**

VI. GAPS AND UNVERIFIED

- The Check Point campaign's actor and the identities of the wiped Israeli victims are unknown. Check Point Research leaves several scenarios open.
- Microsoft's root-cause wording comes through a customer status page and Reuters. No public post-incident report has been read.
- The cause of Monadnock's outage is unconfirmed. Vanderbilt has not confirmed any data theft.
- Ransomware.live counts use UTC dates and are backfilled. gpsjam and AIID were not refreshed today.

Sources

CISA KEV, alerts and directives; Check Point support and Check Point Research; ransomware.live; Monadnock Community Hospital; Vanderbilt News; SEC EDGAR; Microsoft 365 status; Reuters (Investing.com); University of Queensland ITS status; Federal Register; Euronews; Chemical Week; Washington Examiner; php.net; php-src on GitHub.