



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 33 | 2 August – 8 August 2026

THREAT LEVEL: HIGH

TLP:WHITE

Report ID: SA-CTI-2026-W33 | Classification: TLP:WHITE

Published Monday 10 August 2026

Compiled by Willem Steynberg – <https://www.linkedin.com/in/willem-steynberg-8a52234/>

Reviewed by Percy Kitso Sekate – <https://www.linkedin.com/in/percy-kitso-sekate/>

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard**
- 2. Threat Landscape Heatmap**
- 3. Top SA Incidents (W33)**
- 4. Threat Actors**
- 5. Critical Vulnerabilities & CISA KEV**
- 6. Ransomware Landscape**
- 7. OSINT Exposure & Attack Surface**
- 8. Regulatory & Policy**
- 9. Weekly Threat Hunt & IOCs**
- 10. Strategic Recommendations**
- 11. Threat Level Assessment**
- 12. OSINT Sources Consulted**



TRAIN LIKE AN ATTACKER. LEVEL UP.

Live, virtual, instructor-led hacking courses — **attend online from anywhere.**

Two days per course · 09:00–17:00 (GMT+2) · Taught live by SensePost hackers



0xCD: Hands-On Hacking Fundamentals

Build a solid offensive security foundation, hands-on from day one.

8–9 SEPT
2026



0xCD: Pragmatic API Exploration

Everything is an API: Learn to explore, test and exploit them.

22–23 SEPT
2026



0xCD: Web Application Hacking

Sharpen your web app testing skills against real-world style targets.

6–7 OCT
2026

- » Individual lab access for each person joining the training
- » Taught by ethical hackers with current field experience
- » Practical-driven learning through guided tasks, hands-on labs, and real-world style challenges
- » Content grounded in real methodologies and client work

»» **BOOK YOUR SEAT** training+sept@orangecyberdefense.com



1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH, 13th consecutive week (2 August - 8 August 2026)

Story 1. A regulated payment distribution agency confirmed a ransomware attack, and it is one of only four in the country. DC Partner (Pty) Ltd confirmed to MyBroadband on 7 August 2026 that it was the victim of a ransomware attack, after the Krybit group listed it on 2 August at 14:25 UTC.¹² This is a confirmed breach, not a leak-site claim. The company says its systems remain fully operational, that its primary concern is discharging its regulatory obligations, that it is issuing notifications under section 22 of POPIA, and that its investigation continues.¹ DC Partner is one of only four National Credit Regulator accredited payment distribution agencies in South Africa, based in George and employing 65 people; its own NCR registration records number NCRPDA02.³¹ A PDA receives one monthly payment from a consumer under debt review and distributes it to that consumer's creditors, so the estate holds identity numbers, bank details, debit order mandates and creditor schedules for people already in financial distress. Krybit claims to have already published the data but has not said where, how much or what it contains, so the scope of any disclosure is unverified.¹ Krybit listed two further South African organisations in the same six days: Buzz Trading 104 (Pty) Ltd trading as Master Products on 2 August at 13:26 UTC, and Serengeti Estates on 7 August at 02:25 UTC. Both remain CLAIMED.²⁴ Before this week Krybit had claimed a single South African victim, in April.

Story 2. Fidelity Services Group confirmed its breach and RansomHouse published the data. On 7 August 2026 Fidelity chief executive Wahl Bartmann confirmed to MyBroadband that the company had suffered a cyber incident, that it had isolated affected systems and engaged specialists, and that it had notified the Information Regulator under section 22 of POPIA. He also said no third-party or customer information was breached.⁵ RansomHouse, which listed the company in mid-July, has since published data it says it took, including what MyBroadband describes as private documents belonging to the chief executive.⁵ This resolves a carryover that W32 rated CLAIMED. The company's position that no customer data was affected and the actor's publication of a dataset cannot be reconciled from open sources, and both are recorded here rather than one being chosen. Fidelity is Southern Africa's largest integrated security provider, running guarding and cash-in-transit operations.

Story 3. INTERPOL published hard numbers on South Africa's share of African cybercrime, and they are worse than this report has previously been able to evidence. On 3 August 2026, inside the window, INTERPOL released its African Cyberthreat Assessment Report 2026, drawn from survey data across 36 African member countries and from Fortinet, Mastercard, the Shadowserver Foundation, S2W and TrendAI.⁶⁷ South Africa accounts for 92 per cent of all ransomware detections in Africa, 70 per cent of business e-mail compromise detections, 43.6 per cent of the vulnerability detections identified by the Shadowserver Foundation, and close to 40 per cent of phishing detections, and recorded 213,523 DDoS attacks, one peaking at 312 Gbps.⁷ Continent wide, AI featured in 55 per cent of cybercrime cases in 2025 and losses more than doubled since 2024, from USD 192 million to USD 484 million.⁶ That AI finding independently corroborates the SARS alert this report reported in W32.

Corrections to Prior Editions

Four corrections are owed to prior editions.

- **Correction 1, to W32.** W32 reported that no South African leak-site claim was dated inside its window and carried a KPI reading zero claims. Both were wrong. DC Partner and Buzz Trading 104 were indexed on 2 August at 14:25 and 13:26 UTC, seven and eight hours after that edition's collection run completed. The window ended at Sunday midnight while collection ran on Sunday morning, so the final sixteen hours were never observed. The window moves to Sunday through Saturday from this edition. The corrected W32 figures are two claims inside the window and a cumulative total of 118, not 116.
- **Correction 2, to W30, W31 and W32.** Those editions reported that the country feed lagged leak-site postings by eleven to fourteen days, quantified in W32 at two to three weeks. That claim is retracted. On 8 August the free country endpoint returned 119 South African records and on 9 August the API victims endpoint returned the same 119, with identical timestamps on all three window victims. The lag was asserted across three editions without a measurement capable of distinguishing a feed delay from a collection defect, and the defect in Correction 1 is the better explanation.
- **Corrections 3 and 4, to W32 and W31.** SuppCenter Global Services and Recsa, reported as South African listings, are neither of them South African. The actor's own post describes SuppCenter as a Latin America regional partner and carries a +506 Costa Rica number, and the aggregator holds that victim twice with identical descriptions, tagged Argentina and South Africa. Recsa is tagged Costa Rica with the domain www.recsa.com, a Latin American collections group; the South African attribution originated in a single secondary article that matched the name to the Regional Centre on Small Arms in Nairobi, of which South Africa is not a member. Both entered through a secondary layer that rewrites the aggregator's country field without checking it, and both resolve to Costa Rica. A country tag on an aggregated leak-site record is not evidence of nationality. Both entities are removed from tracking.

KPI Dashboard

Metric	Current (W33)	Prior (W32)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (13th week)	FLAT
ransomware.live SA cumulative	119	118 (corrected from 116)	+1	UP
SA claims dated inside the window	3	2 (corrected from 0)	+1	UP
SA breaches confirmed by the victim	2	0	+2	UP
New CISA KEV additions	6	3	+3	UP
KEV adds already overdue at publication	5	2	+3	UP
KEV adds with a VERIFIED SA exposure figure	2 of 6	n/a (metric added W33)	new metric	FLAT
Corrections issued to prior editions	4	0	+4	UP
Weeks since last IR publication	10	9	+1	UP

W33 KEY FRAMING: this was the week the domestic and the international picture said the same thing from two directions. Two South African organisations confirmed breaches, one of them a regulated payment distribution agency holding the banking details of consumers under debt review, while INTERPOL put South Africa at 92 per cent of Africa's ransomware detections and SABRIC put digital banking crime losses at R2.4 billion. Neither observation is new in kind; what is new is that the second is now sourced to an international law enforcement body rather than inferred from a leak-site count. For a South African board the useful reading is that this country is where the African share of ransomware lands, and that a week producing two victim confirmations produced no regulatory statement at all. Technically the week was about deadlines rather than novelty: six KEV additions, five expired before this report reached a reader, two of them the same N-able N-central weakness patched twice. The exploited surface also moved inward, away from the perimeter appliances that have dominated since W30 and towards the software that manages estates and builds code.

TOP 3 ACTIONS THIS WEEK

1. Patch N-able N-central to Hotfix 2, build 2026.3.1.10, on Tuesday 11 August, the first working day after publication, and treat any unpatched instance as compromised. N-able observed exploitation from 1 August, published Hotfix 1 on 2 August, then a second hotfix on 6 August. Huntress measured 28.6 per cent of reachable self-hosted servers still unpatched during the window. Hunt for a Windows service named Cloudflared, a svchost.exe under a user's Documents folder, and Take Control sessions logged as MSP Support in Windows Application Event IDs 4102, 8192 and 8193. Two of the ten addresses N-able published are commercial VPN exit nodes, so correlate rather than block and forget. If you buy IT services from a managed service provider, ask them in writing this week whether they run N-central and whether Hotfix 2 is applied.

2. If you are a credit provider, debt counsellor or bank with debit order exposure to a payment distribution agency, act on the DC Partner breach now. The company has confirmed the attack and is issuing section 22 notifications, and the actor claims to have published data. Review debit order instructions originating from PDA files, raise the threshold for changes to banking details communicated by e-mail, and warn consumers under debt review that they may receive convincing approaches quoting their real payment arrangements. Debt review consumers are an unusually exploitable group because they already expect unfamiliar parties to contact them about money, and they are least able to absorb a loss.

3. Find the Apache Tomcat cluster port before assuming you are exposed, then deal with Langflow. There are 776 internet-facing Tomcat instances in South Africa, but CVE-2026-34486 is not reachable through the web port. It is reachable through the Tribes clustering receiver on TCP 4000, and only where clustering is enabled with the EncryptInterceptor configured and deserialisation gadget classes on the classpath. Hunt for exposed 4000 rather than treating all 776 as vulnerable, and upgrade to 11.0.21, 10.1.54 or 9.0.117. Langflow is the opposite case: CVE-2026-9198 needs no credentials and works against default deployments, there are 32 instances exposed in South Africa, and 650 exploitation attempts from 244 addresses have been recorded since 6 July. Upgrade to 1.10.1 and take it off the public internet.

1. MyBroadband, SA payment distribution agent for FNB and the NCR hit by data breach (7 August 2026). <https://mybroadband.co.za/news/security/661578-south-african-payment-distribution-agent-for-fnb-and-the-national-credit-regulator-hit-by-cyberattack.html>

2. Ransomware.live, SA victim records via the API victims endpoint, 119 records, purity 1.0 (retrieved 9 August 2026). <https://www.ransomware.live/map/ZA>

3. DC Partner, NCR Registration: number NCRPDA02, one of four registered PDAs in SA (retrieved 9 August 2026). <https://www.dcpartner.co.za/NCR-Registration>

4. Ransomware.live, Victim record: Serengeti Estates / Krybit (discovered 7 August 2026). <https://www.ransomware.live/id/d3d3LnNlcmVuZ2V0aWVzdGF0ZXMuY28uemFAa3J5YmI0>

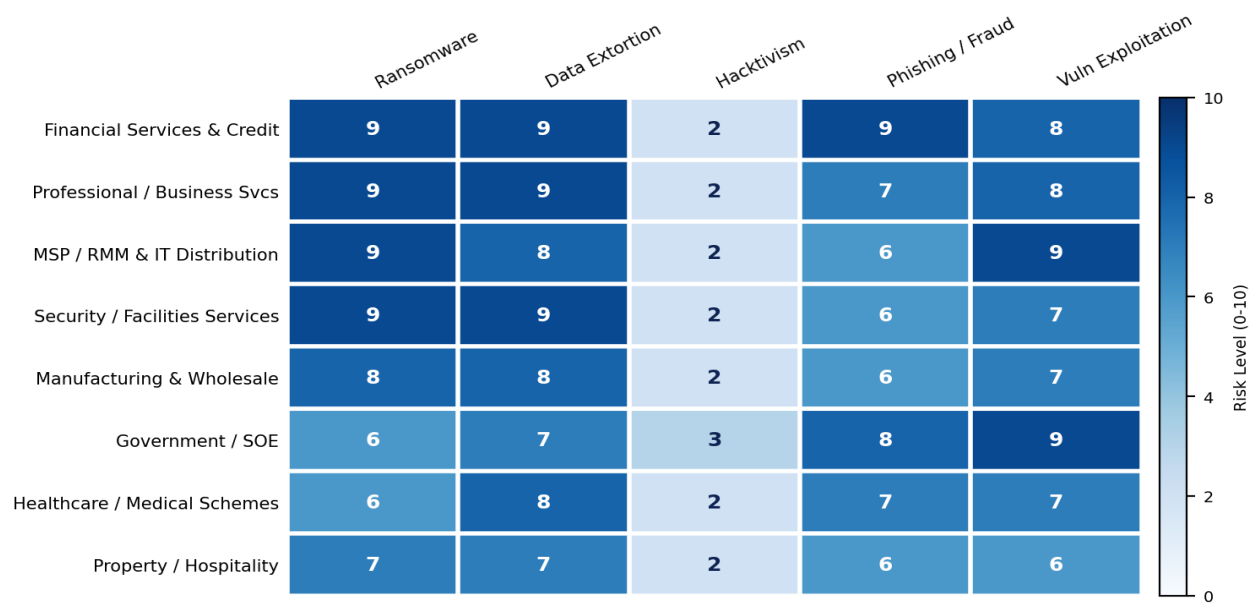
5. MyBroadband, SA's largest private security company suffers data breach (7 August 2026). <https://mybroadband.co.za/news/security/661700-south-africas-largest-private-security-company-suffers-data-breach.html>

6. INTERPOL, INTERPOL report finds AI linked to more than half of cybercrime in Africa (3 August 2026). <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa>

7. INTERPOL, African Cyberthreat Assessment Report 2026 (released 3 August 2026; 36 member countries). <https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W33 (2 - 8 August 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting window; (b) credible threat-actor claims against sector entities; (c) exposure to vulnerabilities under active exploitation; and (d) sector-specific regulatory and operational pressure. Critical 9-10 = active exploitation or confirmed breach; High 7-8 = credible active threat; Medium 4-6 = elevated baseline; Low 1-3 = standard posture. A row added this week enters at a value; it does not rise to one.

Four rows change. **MSP / RMM and IT Distribution**, **Professional and Business Services**, **Manufacturing and Wholesale** and **Property and Hospitality** enter, replacing Retail, Energy and Resources, Engineering and Professional Services and MSSP / Supply Chain. Energy and Resources is retired with the Reatile Group claim still open, which is tracked in Section 3 rather than on the chart. A row that enters does so at a value; it does not rise to one. **MSP / RMM and IT Distribution** enters at 9 on Ransomware and 9 on Vulnerability Exploitation. The driver is the N-able N-central pair, remote monitoring and management software under confirmed exploitation whose compromise reaches downstream customers by design, with Huntress observing one compromised partner instance used to reach nine downstream organisations.⁸ Rectron remains an unresolved South African IT distribution breach in the same category. **Financial Services and Credit** rises to 9 across Ransomware, Data Extortion and Phishing and Fraud on the confirmed DC Partner breach and SABRIC's R2.4 billion figure.¹⁹ **Professional and Business Services** rises to 9: DC Partner is tagged to that sector, and professional services is the largest slice of Krybit's own victim distribution at 21.4 per cent.¹⁰ **Security and Facilities Services** holds at 9, now on a confirmed breach with published data rather than a claim.⁵ **Property and Hospitality** rises on the Serengeti Estates listing.⁴ **Hacktivism** stays low at 2 to 3: no South African hacktivist activity was observed.

3. TOP SA INCIDENTS (W33)

Week 33 recorded three South African leak-site listings dated inside the window, all by the same actor, and two victim confirmations. Two of the three listings are the ones missed by the previous edition and corrected in Section 1. Incidents 3.1 to 3.3 are presented in order of assessed significance. 3.1 is rated **CONFIRMED** on the victim's own statement to national media; 3.2 and 3.3 remain **CLAIMED**, each resting on a threat-actor posting with no victim statement located. This report does not treat an actor assertion as a breach.²

3.1 INC-2026-W33-01: Krybit Ransomware at DC Partner, NCR-Accredited Payment Distribution Agency [CONFIRMED]

Sector	Financial Services and Credit Infrastructure (www.dcpartner.co.za)
Date	Listed by the actor 2 August 2026 14:25 UTC; victim confirmation published 7 August 2026
Confirmed	Yes. DC Partner confirmed the ransomware attack to MyBroadband; systems reported fully operational; section 22 POPIA notifications being issued; investigation ongoing
Victim profile	One of only four National Credit Regulator accredited payment distribution agencies in South Africa. NCR number NCRPDA02, appointed 2008 and registered under the National Credit Act in 2016. Based in George, Western Cape, 65 employees
Data at risk	Identity numbers, bank account details, debit order mandates, creditor schedules and payment histories for consumers under debt review
Actor claim	Krybit states on its leak site that it has already published the stolen data, but does not state where, how much, or what the dataset contains. Scope of any disclosure is UNVERIFIED
Confidence	CONFIRMED (victim confirmation to national media; regulatory notification under way)

Krybit listed www.dcpartner.co.za on 2 August 2026 at 14:25 UTC, and DC Partner confirmed the attack to MyBroadband five days later.²¹ The company's account is measured: systems remain fully operational, its primary concern is discharging its regulatory obligations, and it is currently sending section 22 notifications while its investigation continues.¹ The role of the business is what makes this the week's most consequential item, and it is corroborated twice over: DC Partner's own NCR registration page records number NCRPDA02 and states it is one of only four registered payment distribution agencies in the country, and MyBroadband reports the same status.³¹ A PDA sits between an over-indebted consumer and that consumer's creditors: one payment goes in each month and is split according to a negotiated or court-ordered schedule. The estate therefore holds exactly the material that makes convincing financial social engineering possible, namely correct balances, instalments, creditors and bank details, attached to people least able to absorb a loss. MyBroadband reports the company's software integrates with debt counselling platforms including Finwise, iDOCS, Legacies and DREX, and with FNB's DebiCheck.¹ That describes an integration surface and nothing more: no reporting suggests any of those platforms was affected. Krybit's claim to have already leaked the data should be treated as unverified until a dataset is located.² **TTPs:** no vendor has attributed an initial access vector to any Krybit intrusion, including this one. The techniques associated with the group as a whole are T1078 Valid Accounts and T1021.001 Remote Desktop Protocol.¹⁰ **Detection relevance:** TH-2026-W33-01 carries the Krybit indicators;

TH-2026-W33-06 covers the downstream debt review fraud risk, which a confirmed breach makes materially more likely.

3.2 INC-2026-W33-02: Krybit Claims Buzz Trading 104 (Pty) Ltd, trading as Master Products [CLAIMED]

Sector	Manufacturing and Wholesale (www.buzztrading104.co.za). Note: the aggregator tags this record Financial Services, which appears to be a mis-tag given the actor's own description
Date	Leak-site listing 2 August 2026 13:26 UTC
Claimed	Data theft. No ransom figure stated, no data published, no dataset located
Victim profile	South African privately owned manufacturer and wholesaler, per the actor's own description of the company
Confidence	CLAIMED (threat-actor assertion only; no victim statement located)

Krybit listed Buzz Trading 104 an hour before DC Partner on the same afternoon.² No public statement has been located, no data has been published, and no ransom figure appears in the listing. The record is reported here because it is one of the two listings the previous edition missed. One methodological point is worth carrying: the aggregator classifies this victim as Financial Services while the actor's own description calls the company a manufacturer and wholesaler. This report has now found two separate categories of error in that metadata in one week, the other being the country field in Corrections 3 and 4, so sector and country fields on these feeds should be treated as leads rather than facts. **TTPs:** none observed or published for this intrusion; the group-level techniques in 3.1 apply. **Detection relevance:** TH-2026-W33-01.

3.3 INC-2026-W33-03: Krybit Claims Serengeti Estates [CLAIMED]

Sector	Property and Hospitality (www.serengetiestates.co.za). Aggregator sector field returns Not Found
Date	Leak-site listing 7 August 2026 02:25 UTC
Claimed	Data theft. No ransom figure stated, no data published
Victim profile	Serengeti Golf and Wildlife Estate, a residential golf and wildlife estate
Confidence	CLAIMED (threat-actor assertion only; no victim statement located)

The third Krybit listing of the window arrived on 7 August.⁴ No statement has been located. The reason it earns a place rather than a line in a table is the holding profile of the victim type. A residential estate maintains access control records, biometric enrolments, vehicle registrations and resident contact information, which converts a data breach into a physical security exposure for residents who are third parties to the incident. This is the second time in four weeks that a South African listing in consecutive editions has carried that property, the other being Fidelity Services Group, and it argues for treating physical security and facilities data as a distinct category of personal information. **TTPs:** none observed or published for this intrusion; the group-level techniques in 3.1 apply. **Detection relevance:** TH-2026-W33-01.

Carryover Status (checked 9 August 2026)

Fidelity Services Group and RansomHouse: RESOLVED, now CONFIRMED, data published. Chief executive Wahl Bartmann confirmed the incident on 7 August, the Information Regulator was notified under section 22, and RansomHouse has published data including what MyBroadband describes as private documents of the chief executive.⁵ The company states no third-party or customer information was breached while the actor has published a dataset; those positions cannot be reconciled from open sources and both are recorded. MyBroadband dates the listing to 12 July while the aggregator records discovery on 15 July with an estimated attack date of 12 July, so it is best described as 12 to 15 July.⁵² The possible-duplicate flag against a 28 June listing by a different group remains unresolved. **AVBOB: RESOLVED, promoted from UNDETERMINED to CONFIRMED.** AVBOB's published FAQ discloses a breach identified on 30 May 2026 affecting policyholders, employees and suppliers, and states the Information Regulator and all affected parties were notified under POPIA. That closes an item undetermined for ten weeks. No leak-site listing exists for AVBOB. **Isegen and DragonForce: RESOLVED, and the resolution is a negative.** The actor's 6 August publication deadline for the claimed 234.63 GB fell inside this window and passed with nothing published, while DragonForce posted two other victims that same day. This is non-publication, not operator inactivity, and Isegen's denial stands. **Rectron: no development in the window.** The incident ran 14 to 27 July, the Information Regulator was notified, Mustek filed a SENS announcement on 22 July, and IT-Online reported on 27 July that all branches had reopened.¹¹ No leak site names Rectron. **CKR Consulting Engineers and BE Travel:** BlackFog's July round-up, published 4 August, records the Payload claim of 55 GB against CKR, which has not responded, and records BE Travel confirming its incident and notifying individuals under POPIA. The Arcus Media deadline against BE Travel lapsed on 21 July with nothing published.¹² **Reatile Group, Profmed and PPS Healthcare Administrators, the Gauteng e-Government jobs portal, and Standard Bank and Liberty via Prinz Eugen: no development found;** the Standard Bank listing remains live and unretracted.² **Removed from South African tracking:** SuppCenter Global Services and Recsa, per Corrections 3 and 4.

10. SOCRadar, Dark web profile: Krybit ransomware. <https://socradar.io/blog/dark-web-profile-krybit-ransomware/>

11. IT-Online, Rectron's doors reopen (27 July 2026). <https://it-online.co.za/2026/07/27/rectrons-doors-reopen/>

12. BlackFog, The State of Ransomware: July 2026 (4 August 2026; CKR and BE Travel entries). <https://www.blackfog.com/the-state-of-ransomware-july-2026/>

4. THREAT ACTORS

4.1 Krybit: One Actor, Three South African Victims in Six Days

Krybit emerged on 31 March 2026 as a ransomware-as-a-service operation. Affiliates keep 80 per cent of ransom payments and the operator keeps 20, and builders are provided for Windows, Linux, VMware ESXi and NAS devices.¹³¹⁰ The model is double extortion: data is exfiltrated ahead of encryption, reportedly 10 to 250 GB per victim, then files are encrypted with the .KRYBIT extension appended and a RECOVER-README.txt note dropped in each affected directory.¹³¹⁴ Antivirus engines identify a captured sample as a Babuk derivative, detected by ESET as Win32/Filecoder.Babuk.A, by Microsoft as Trojan:Win32/Babuk!ic and by Combo Cleaner as Generic.Ransom.Babuk.!s!.G.2B7CD25C.¹⁴ SOCRadar makes the caveat that matters alongside that finding: such detections are consistent with the large

population of families built on the leaked 2021 Babuk source rather than with bespoke engineering, so lineage is a fact about code provenance and not an attribution.¹⁰ DeXpose reported the DC Partner listing on 3 August and quoted the actor's demand that a representative make contact.¹⁵ No CVE exploitation has been attributed to Krybit by any vendor, and no specific phishing lure or exposed service has been publicly tied to any of its intrusions; the techniques associated with the group are T1078 Valid Accounts and T1021.001 Remote Desktop Protocol.¹³¹⁰

In April 2026 Krybit fought a public feud with the rival group OAPT, which leaked Krybit's admin panel on 13 April before Krybit reached OAPT's servers and published its data in turn.¹⁶ That leaked panel is the reason unusually detailed indicators exist for this group: two operators and five affiliates, ransom demands of USD 40,000 to USD 100,000, and five Bitcoin wallets that showed no transactions at the time.¹⁶ Those identifiers are carried in Section 9 and the indicator export.

Krybit claimed one South African victim between March and July. It claimed three in the six days from 2 to 7 August.² **A wider African pattern is visible in the same data, and this is the report's own observation rather than published vendor research.** Krybit's victim list includes a college in Botswana, a life assurer in Zambia, a hospital in Kenya, the Cour des Comptes in Senegal which is a national supreme audit institution, a mutual society in Morocco, the state-owned Nile Petroleum in South Sudan, and a Nigerian microfinance bank listed on 2 August, the same day as the two South African claims. No vendor has written that cluster up. Read alongside INTERPOL's finding that South Africa absorbs 92 per cent of African ransomware detections, it suggests an affiliate base that has found African targets productive.⁷ Globally the group claims roughly 90 to 100 victims across more than 40 countries with no regional concentration, weighted towards smaller organisations.

4.2 Actors Behind the Week's Exploitation

The N-able N-central intrusions are unattributed. N-able describes post-compromise use of the built-in Take Control feature and a Cloudflare Tunnel registered as a Windows service for persistence, while Huntress, examining the same activity independently, saw process enumeration and disconnection and did not observe the Cloudflare installation.¹⁷⁸ That divergence is recorded rather than resolved. For Apache Tomcat, Unit 42 attributes attempted exploitation of CVE-2026-34486 against nine servers to a Chinese-speaking actor operating an AI agent framework manually, listing it under attempts with no confirmed success.¹⁸ JetBrains TeamCity has no published victimology at all.

13. Halcyon, KryBit threat group profile (RaaS from March 2026; affiliate model; sample hash). <https://www.halcyon.ai/threat-group/krybit>

14. PCrisk, Krybit ransomware analysis (.KRYBIT extension, RECOVER-README.txt). <https://www.pcrisk.com/removal-guides/35210-krybit-ransomware>

15. DeXpose, Krybit ransomware targets DC Partner in South Africa (3 August 2026). <https://www.dexpose.io/krybit-ransomware-targets-dc-partner-in-south-africa/>

16. Halcyon, OAPT vs KryBit: actors list opposing operators as victims (April 2026). <https://www.halcyon.ai/ransomware-research-reports/Oapt-vs-krybit-ransomware-actors-list-opposing-operators-as-victims>

5. CRITICAL VULNERABILITIES & CISA KEV

Six vulnerabilities entered the CISA KEV catalogue between 2 and 8 August 2026, against three the previous week, and five of the six were past their remediation date before this report reached a reader.¹⁹ CISA added CVE-2026-18577 on 3 August, then CVE-2026-18556, CVE-2026-34486 and CVE-2026-9198 on 4 August, CVE-2026-63077 on 5 August and CVE-2026-8037 on 7 August. Only Progress LoadMaster was still inside its deadline, which expired on Monday 10 August.¹⁹ That date is a public holiday in South Africa, Women's Day having fallen on Sunday 9 August, so most local teams will first read this on Tuesday 11 August with the LoadMaster deadline behind them and every other item a day deeper overdue. Plan the week on that basis rather than on the catalogue dates. Two of the six are the same weakness in the same product: CISA records CVE-2026-18577 as the result of an incomplete patch for CVE-2026-18556, and N-able issued a second hotfix on 6 August after the first.¹⁹¹⁷ All six carry a knownRansomwareCampaignUse value of Unknown, which is weaker than an assertion that ransomware operators are not using them. As in recent editions, KEV remediation dates are set per entry rather than on a uniform interval, so a fixed interval in a patch-management SLA will produce false compliance.¹⁹

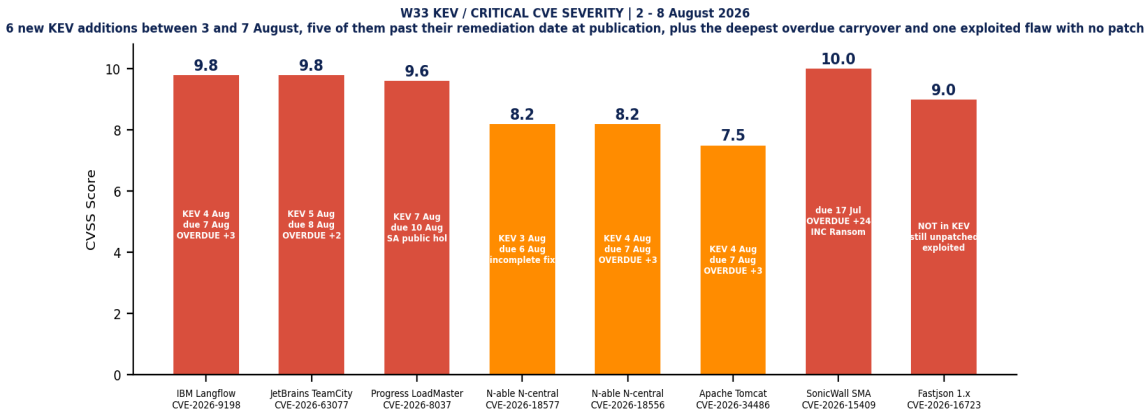
N-able N-central, CVE-2026-18556 and CVE-2026-18577. Both are authentication bypasses using an alternate path or channel, giving an unauthenticated remote attacker administrative control. N-able has published no root cause or exploit primitive, so none is described here. The sequence matters more than the mechanism: N-able fixed the first path in release 2026.2, then found another route to the same weakness that the fix did not block, which became CVE-2026-18577. Hotfix 1 shipped on 2 August and Hotfix 2 on 6 August with what the vendor calls additional hardening.¹⁷²⁰ N-able declined to tell The Register whether attackers had bypassed Hotfix 1, so whether exploitation defeated the first fix is unresolved.²¹ Exploitation has been observed since 1 August. Huntress reports one self-hosted instance in a single partner account used to reach nine downstream organisations, and measured 28.6 per cent of reachable self-hosted servers still unpatched during the window; it notes the appliance runs a custom Linux build that frequently carries no endpoint detection at all.⁸

Apache Tomcat, CVE-2026-34486. A fail-open regression introduced by the fix for an earlier flaw: the refactor moved the call that forwards a message outside the block handling decryption failure, so a message that fails to decrypt is logged and then forwarded into deserialisation with no class filter.²² The preconditions are what keep the South African exposure figure honest: Tribes clustering enabled, the EncryptInterceptor configured, the receiver on TCP 4000 reachable, and gadget classes on the classpath. Versions 11.0.19 to 11.0.20, 10.1.53 and 9.0.116 are affected; 11.0.21, 10.1.54 and 9.0.117 fix it.²² The KEV note that this chains with CVE-2025-24813 is CISA's characterisation and no primary analysis demonstrating the two used together could be located, so it is reported as a catalogue assertion.¹⁹ **IBM Langflow, CVE-2026-9198.** In default deployments one endpoint issues a superuser token to any unauthenticated caller and another then executes attacker-supplied Python. Versions 1.0.0 to 1.10.0 are affected, 1.10.1 fixes it, and no workaround exists.²³ Telemetry cited by The Hacker News records 650 exploitation attempts from 244 addresses across 41 countries since 6 July.¹⁸ This is the second Langflow remote code execution flaw to enter KEV in weeks.

JetBrains TeamCity, CVE-2026-63077, is unsafe XStream deserialisation reachable before authentication through the agent polling endpoints, affecting all On-Premises versions.²⁴ One honesty point belongs on the record: JetBrains reported no known exploitation at disclosure on 27 July, and the in-the-wild claim

rests solely on the KEV addition of 5 August, with no victimology or attacker infrastructure published.²⁵ **Progress LoadMaster, CVE-2026-8037**, is an uninitialised heap allocation and missing null terminator in the request-escaping routine, reachable through /accessv2 when the API is enabled.²⁶ eSentire observed attempts from 29 June, all of which failed, and separate telemetry records 792 attempts over 41 days from 65 addresses, last seen 4 August.²⁷¹⁸ No confirmed compromise has been reported by any source.

W33 KEV / Critical CVE Severity Overview: 6 New KEV Adds Plus Overdue and Unpatched Items



W33 CISA KEV / Critical CVE Tracking (new adds 3-7 August plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-18577	N-able N-central	8.2	Auth bypass	6 Aug	KEV 3 Aug. OVERDUE +4. Incomplete patch for CVE-2026-18556. Hotfix 2 build 2026.3.1.10 is mandatory even after Hotfix 1. Ransomware use: Unknown.
CVE-2026-18556	N-able N-central	8.2	Auth bypass	7 Aug	KEV 4 Aug. OVERDUE +3. Exploited from 1 Aug. One partner instance reached nine downstream organisations. Appliance often carries no EDR.
CVE-2026-9198	IBM Langflow	9.8	Code injection (unauth RCE)	7 Aug	KEV 4 Aug. OVERDUE +3. Default deployments: auto_login issues a superuser token, validate/code executes Python. Fixed 1.10.1. 32 exposed in ZA. EPSS 0.1705.

CVE-2026-34486	Apache Tomcat	7.5	Missing encryption (fail-open)	7 Aug	KEV 4 Aug. OVERDUE +3. Reachable via Tribes clustering on TCP 4000, NOT the web port. Fixed 11.0.21 / 10.1.54 / 9.0.117. EPSS 0.8116.
CVE-2026-63077	JetBrains TeamCity	9.8	Deserialisation (unauth RCE)	8 Aug	KEV 5 Aug. OVERDUE +2. Pre-auth XStream deserialisation via agent polling. Fixed 2025.11.7 / 2026.1.3. In-the-wild claim rests solely on the KEV listing. EPSS 0.0101.
CVE-2026-8037	Progress LoadMaster	9.6	Command injection (pre-auth)	10 Aug	KEV 7 Aug. Due on publication day. Uninitialised heap via /accessv2. Fixed GA 7.2.63.2 / LTSF 7.2.54.18. Attempts only, no confirmed compromise. EPSS 0.9931.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	OVERDUE +24, the deepest carryover tracked. INC Ransomware is now reported as the dominant actor on this chain. Credentials, active sessions and TOTP seeds are stolen, so rebuild the appliance rather than patch it.
CVE-2026-46817	Oracle E-Business Suite	n/a	Improper privilege mgmt	18 Jul	OVERDUE +23. Re-verify against the 21 July Critical Patch Update. NVD gives 9.8.
CVE-2026-16723	Alibaba Fastjson 1.x	n/a	Unauth RCE (deserialisation)	n/a	STILL NOT IN KEV, still unpatched on 1.x. Exploitable in default config 1.2.68-1.2.83. Migrate to 2.x or set fastjson.parser.safeMode=true. No confirmed victim.

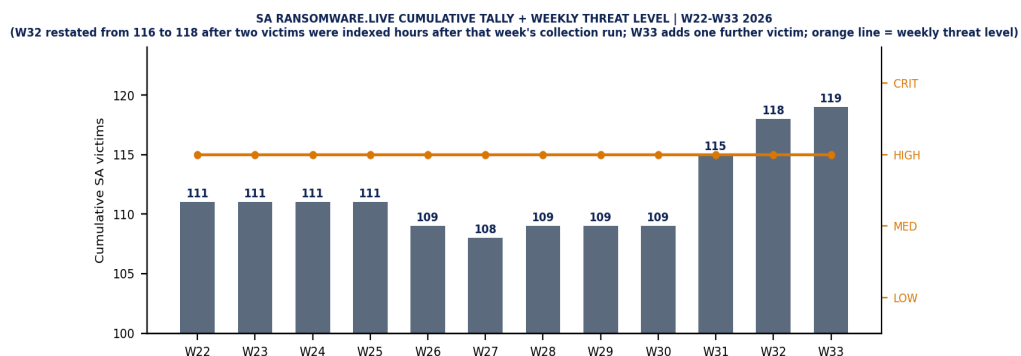
Pattern note: two of the six additions are the same weakness in the same product, patched twice, in software whose entire purpose is remote administrative control of other people's computers. Three of the six are developer and automation infrastructure rather than perimeter appliances. The edge-device story running since W30 has not gone away, and SonicWall is now twenty-four days overdue with reporting this week naming INC Ransomware as the dominant actor on that chain,²⁸ but the newly exploited surface moved inward this week, to the tools that manage estates and build software, typically stood up by developers rather than provisioned by IT. On EPSS: TeamCity scores 0.0101 and the second N-central entry 0.0049 while both are listed as exploited. EPSS predicts the next thirty days and lags confirmed activity, so it must never be used to deprioritise a KEV entry.

8. Huntress, N-able N-central vulnerability exploitation (3 August 2026). <https://www.huntress.com/blog/n-able-vulnerability-exploitation>

17. N-able, N-central security update (6 August 2026; Hotfix 2 build 2026.3.1.10; attacker IP list). <https://www.n-able.com/blog/n-central-security-update-august-6-2026>
18. The Hacker News, CISA flags Langflow RCE, Tomcat and N-central flaws (August 2026). <https://thehackernews.com/2026/08/cisa-flags-langflow-rce-tomcat-and-n.html>
19. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.07 (retrieved 9 August 2026). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
20. Rapid7, CVE-2026-18577 N-able N-central auth bypass exploited in the wild (2 August 2026). <https://www.rapid7.com/blog/post/etr-cve-2026-18577-n-able-n-central-authentication-bypass-exploited-in-the-wild/>
21. The Register, N-able confirms attackers reached customer networks as second hotfix lands (7 Aug 2026). <https://www.theregister.com/2026/08/07/n-able-god-mode-flaw-vendor-confirms-attackers-reached-customer-networks-as-second-hotfix-lands/5284730>
22. Striga, Apache Tomcat Tribes unauthenticated RCE, CVE-2026-34486 technical analysis. <https://www.striga.ai/research/tomcat-tribes-unauth-rce>
23. IBM, Security Bulletin: Langflow code injection CVE-2026-9198 (fixed in 1.10.1). <https://www.ibm.com/support/pages/node/7278927>
24. Rapid7, Unauthenticated RCE in JetBrains TeamCity, CVE-2026-63077 (7 August 2026). <https://www.rapid7.com/blog/post/ra-unauthenticated-rce-in-jetbrains-teamcity-cve-2026-63077/>
25. SecurityWeek, Hackers start exploiting recent JetBrains TeamCity vulnerability (August 2026). <https://www.securityweek.com/hackers-start-exploiting-recent-jetbrains-teamcity-vulnerability/>
26. watchTowr Labs, Progress Kemp LoadMaster uninitialized heap to pre-auth RCE, CVE-2026-8037. <https://labs.watchtowr.com/enterprise-tech-in-shell-out-progress-kemp-loadmaster-uninitialized-heap-to-pre-auth-rce-cve-2026-8037/>
27. eSentire, Progress Kemp LoadMaster targeted, CVE-2026-8037 (attempts from 29 June 2026). <https://www.esentire.com/security-advisories/progress-kemp-loadmaster-vulnerability-targeted-cve-2026-8037>
28. The Hacker News, INC Ransomware emerges as dominant actor on the SonicWall SMA chain (August 2026). <https://thehackernews.com/2026/08/inc-ransomware-emerges-as-dominant.html>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 119 records when retrieved at 07:21 UTC on 9 August 2026, with a client-side country filter purity of 1.0.² Three of those records are dated inside this window and all three belong to Krybit. Against the figure this report published in W32, 116, the movement is +3, and it decomposes into two corrections and one genuinely new listing rather than three new victims. DC Partner and Buzz Trading 104 were indexed on 2 August, hours after the previous edition's collection run, and are counted here as corrections to that edition; Serengeti Estates on 7 August is the only listing that is new in the ordinary sense. The corrected W32 baseline is therefore 118 and the W33 closing figure is 119. This edition also retires the aggregator-lag claim carried in W30, W31 and W32: the free country endpoint on 8 August and the API victims endpoint on 9 August both returned 119 records with identical timestamps on all three window victims, which is not the behaviour of a feed running two to three weeks behind.² The collection defect described in Correction 1 accounts for what was previously attributed to the feed.



Baseline (W32, corrected)	118 cumulative SA victims. W32 published 116; two victims indexed on 2 August after that edition's collection run are corrected into the baseline
Current (W33)	119 cumulative SA victims, retrieved 9 August 2026 07:21 UTC, filter purity 1.0
Claims dated inside the window	3, all Krybit: Buzz Trading 104 (2 August 13:26 UTC), DC Partner (2 August 14:25 UTC), Serengeti Estates (7 August 02:25 UTC)
Delistings or restorations	None observed
Delta explanation	+3 against the figure W32 published, of which 2 are corrections and 1 is a new listing. Against the corrected baseline of 118 the movement is +1
Cross-tier confirmation	The free country endpoint (8 August) and the API victims endpoint (9 August) returned the same 119 records with identical victim timestamps. The lag claimed in W30 to W32 is retracted
Confirmations in window	2. DC Partner confirmed its ransomware attack and Fidelity Services Group confirmed its cyber incident, both reported 7 August 2026
Threat-level drivers	A confirmed breach at regulated payment infrastructure; a confirmed breach with data published at the largest regional security provider; three claims in six days from one actor; five KEV additions overdue at publication; MSP management software under active exploitation

Group notes: **Krybit** accounts for all three listings dated in the window and is profiled in Section 4.1. **RansomHouse** moved from claim to publication against Fidelity Services Group, which is the first time in this series that a South African dataset claimed by an actor has demonstrably been released.⁵ **DragonForce, Arcus Media and Payload** share the opposite property, and it is worth one sentence: DragonForce let its 6 August Isegen deadline pass without publishing, Arcus Media never published against BE Travel after its 21 July deadline lapsed, and Payload has published nothing against CKR Consulting Engineers. Three lapsed deadlines against South African victims without publication is a data point about actor capability or intent, and it is the counterweight to reading every leak-site countdown as imminent. **INC Ransomware** is noted in the Section 5 tracking table. **Prinz Eugen and ROOTBOY:** the Standard Bank and Liberty listing is unchanged and unretracted.²

7. OSINT EXPOSURE & ATTACK SURFACE

South African internet-facing exposure, retrieved 9 August 2026

The figures below count instances of a product family that are internet-facing in South Africa. They are exposure counts and not vulnerability counts: no version filter is applied and none of these numbers says how many instances are unpatched.²⁹ Only fingerprints corroborated by their own product facet are published. **Fortinet FortiGate 1,953. Citrix Netscaler 98. Cisco ASA WebVPN 327. Microsoft SharePoint on-premises 357. WordPress 297. Remote Desktop Protocol on port 3389, 8,186. Services on port 445, 5,124. SonicWall SSL-VPN 13, with the wider SonicWall product family at 2,532. Apache Tomcat 776. Langflow 32.** Each carries its caveat: the WordPress figure is a floor because component detection undercounts; the port 445 figure counts services on that port rather than identified SMB servers; and the SonicWall SSL-VPN figure cannot be narrowed to the SMA 1000 line that carried CVE-2026-15409, so it

must never be read as an SMA 1000 count.

Two figures are new this week, and two of the week's KEV products cannot be measured at all

The Apache Tomcat and Langflow counts are the first exposure figures this report has been able to publish for vulnerabilities added to KEV in the same week they were added.²⁹ They should be read very differently from one another. The 776 Tomcat instances are not 776 vulnerable systems: CVE-2026-34486 is reachable through the Tribes clustering receiver on TCP 4000, not through the web port these instances answer on, and only where clustering is configured with the EncryptInterceptor.²² The right action is to inventory listeners on 4000, not to panic about 776. Langflow is the opposite: 32 is a small number, but CVE-2026-9198 requires no credentials and works against default deployments, so the exposed population and the exploitable population are much closer together.²³ Three of the week's KEV products cannot be measured by this method. JetBrains TeamCity resolves only through a component query whose product facet could not corroborate it, so no figure is published for it. N-able N-central and Progress LoadMaster have no usable fingerprint under any spelling tried. That is a limit of the method and not evidence of absence, and it is worth stating that the one product in this set most likely to matter to South African managed service providers, N-central, is the one that cannot be counted.

Reading these counts over time

These are point-in-time snapshots and not a trend. Two collection runs twenty-two hours apart on 8 and 9 August moved the FortiGate count by 8.6 per cent and one SonicWall product string by 73 per cent with nothing happening in between, which is the scanning platform's rescan cycle rather than South African exposure changing.²⁹ Week-on-week movement in these figures is not a finding unless it is far larger than that noise floor. Per-organisation exposure is deliberately not published: naming an identifiable South African organisation as running an exposed appliance in a document distributed without restriction is targeting information rather than intelligence.

29. Shodan host/count exposure queries for South Africa, VERIFIED fingerprints only (9 August 2026). <https://www.shodan.io/>

8. REGULATORY & POLICY

INTERPOL African Cyberthreat Assessment Report 2026, released 3 August 2026

The assessment draws on survey data from law enforcement in 36 African member countries during 2025, funded by the United Kingdom's Foreign, Commonwealth and Development Office under the African Joint Operation against Cybercrime, with data contributed by Fortinet, Mastercard, the Shadowserver Foundation, S2W and TrendAI.⁶⁷ The South African figures are set out in Section 1. Three further findings matter for governance. First, 89 per cent of surveyed countries cite underreporting as a pervasive challenge, and only Nigeria, Kenya, South Africa and Mauritius mandate breach disclosure within 72 hours.⁷ South Africa's POPIA regime is therefore among the stricter frameworks on the continent, which makes the Regulator's silence below harder to read. Second, 17 countries enacted or amended cybercrime legislation during 2025. Third, four INTERPOL operations produced more than 1,500 arrests and over USD 100 million recovered; Operation Serengeti 2.0 spanned Angola, South Africa and Uganda, dismantling more than 1,200 malicious servers and arresting 120 people.⁶⁷ This report will track INTERPOL publications weekly from this edition forward.

SABRIC 2025 Annual Banking Crime Statistics

SABRIC's 2025 annual statistics were published in the first week of August and reported on 7 August.⁹ Digital banking crime losses reached R2.4 billion in 2025, up from approximately R1.9 billion in 2024, with banking application related crime accounting for more than 70 per cent of reported digital banking losses. Card fraud rose 18 per cent to R1.7 billion. The traditional categories moved the other way: ATM attacks fell 46 per cent, bank robberies fell to two from eight, and fraudulent home loan applications declined 3.4 per cent to R595.9 million.⁹ SABRIC names AI-driven fraud among the emerging threats. Read next to the INTERPOL assessment and the DC Partner confirmation, the week produced three independent measurements of South African financial cyber risk, from a banking industry body, an international police organisation and a regulated payment agency, and all three point the same way.

Information Regulator: ten consecutive weeks without a public statement

The Information Regulator has published no media statement since 2 June 2026.³⁰ That is now ten weeks, and this week it spans two organisations that have confirmed breaches and stated they have notified the Regulator under section 22.¹⁵ The observation is recorded without repeating the argument made in previous editions. The practical consequence for a South African organisation is unchanged: regulatory publication is not a reliable early-warning channel, and breach awareness has to come from elsewhere.

Who to call: South African incident response contacts

POPIA requires notification to the Information Regulator, which is a compliance obligation and not an incident response capability. Six South African teams are listed in the international CSIRT directory.³¹ The two with the broadest constituencies are the **Cybersecurity Hub** (kpillay@cybersecurityhub.gov.za, <https://www.cybersecurityhub.gov.za/>), whose constituency covers government and the private and public sectors, and **ECS-CSIRT** at the State Security Agency (ecs-csirt@ssa.gov.za), covering government and military. Also listed are the **SA NREN CSIRT** (csirt@sanren.ac.za) for research and education, **UCT CSIRT**, **Standard Bank Group CSIRT** and the **Vodacom Group Cyber Intelligence Centre**. Organisations without a retained incident response provider should record the relevant contact in their response plan now rather than looking for it during an incident.

9. Algoa FM, Digital banking crime costs South Africans R2.4bn (7 August 2026; SABRIC 2025 statistics).

<https://www.algoafm.co.za/business/digital-banking-crime-costs-south-africans-r2-4bn-as-fraudsters-target-consumers>

30. Information Regulator (SA), Media statements index; most recent statement 2 June 2026 (checked 9 August 2026).

<https://infoeregulator.org.za/media-statements/>

31. FIRST, South African CSIRT directory: six teams (retrieved 9 August 2026). <https://www.first.org/members/teams/>

9. WEEKLY THREAT HUNT & IOCs

Three P1 missions cover the actor with three South African victims and the two KEV items carrying the richest published forensic detail; two P2 missions cover the remaining exploited software; and one P3 mission covers the downstream fraud risk created by the DC Partner breach, which has no atomic indicators and says so rather than inventing any. The Krybit indicators in TH-01 are drawn from published vendor research.¹³¹⁰¹⁴ A machine-readable export of 59 indicators accompanies this report as iocs_w33.csv.

TH-2026-W33-01: Krybit Ransomware, Three SA Victims in Six Days**P1 CRITICAL:** confirmed SA breach; exfiltration precedes encryption; actor active now

Hypothesis: A Krybit affiliate with South African targeting is operating now. Because the model exfiltrates 10 to 250 GB before encrypting, the earliest reliable signal is bulk outbound transfer rather than an encryption event, and an organisation may be days into an intrusion with no ransomware symptom.

MITRE ATT&CK: T1078 (Valid Accounts), T1021.001 (Remote Services: RDP), T1105 (Ingress Tool Transfer), T1071 (Application Layer Protocol), T1041 and T1567 (Exfiltration), T1490 (Inhibit System Recovery), T1486 (Data Encrypted for Impact), T1562 (Impair Defenses).

IOCs: Sample SHA-256 dab06e47581b87c21699bb1126b7cb2370cf86d069ad25b9b86cff8e450d7e29. Encrypted files gain the .KRYBIT extension; the ransom note is RECOVER-README.txt, indexed by one tracker as README-RECOVER.txt. Shadow copy deletion via 'vssadmin.exe delete shadows /all /quiet'. Five leak-site onions including krybitqsdzwmhntvwuhvsntfgf2wrhxveyxroxc44c6gkft2cqldyd.onion, which hosts the three South African posts. Ransom-note support Tox ID 071EA649F06BDB7123C99653B7371E3B59860EE405E66A31EE0FD385F745A000405B6846ECBC, operator Tox identifiers for the handles KRYBIT and GREP, and five reused Bitcoin wallets, all listed in iocs_w33.csv.

Data Sources: EDR process creation, Windows Event ID 4688, file creation and rename telemetry, netflow and proxy egress logs, backup and volume shadow service logs.

Detection Guidance: Alert on volume shadow copy deletion and on mass file rename to a single new extension. Hunt outbound transfers of 10 GB or more to unfamiliar destinations across the 72 hours preceding any encryption event, since that is where this actor is visible first. The enrichment feed returned no detection rule for this group, so signature coverage has to be built from the artefacts above rather than imported.

TH-2026-W33-02: N-able N-central Auth Bypass and Downstream MSP Reach**P1 CRITICAL:** exploited from 1 Aug; KEV due 6 and 7 Aug (LAPSED); RMM supply chain

Hypothesis: An attacker bypasses authentication on an N-central server, gains administrative control, and uses the built-in Take Control feature to reach managed endpoints at downstream customer organisations. The blast radius is every client on the platform, and the access is difficult to distinguish from legitimate administration because it uses the product's own remote support mechanism.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1219 (Remote Access Software), T1199 (Trusted Relationship), T1572 (Protocol Tunneling), T1036 (Masquerading).

IOCs: A Windows service named Cloudflared, and a svchost.exe located in a user's Documents folder. Windows Application Event IDs 4102, 8192 and 8193 recording a Take Control session, with the malicious session logged under the default username MSP Support. Agent logs at C:\ProgramData\GetSupportService_N-Central\Logs\BASupSrv*_log.gz correlated with the server's ui_access_control.log. Ten attacker addresses published by N-able and three Synology QuickConnect domains, all in iocs_w33.csv.

Data Sources: N-central server logs, Windows Application Event Log on managed endpoints, Take Control agent logs, perimeter netflow, EDR telemetry on the appliance where present.

Detection Guidance: Apply Hotfix 2, build 2026.3.1.10, required even where Hotfix 1 was applied, and treat any instance unpatched during the first week of August as suspected compromised rather than merely exposed. Two cautions on the indicators: two of the ten published addresses are commercial VPN exit nodes, and the listed event IDs also appear in legitimate use, so both are pivots and not proof. If you consume managed services, ask your provider in writing whether they run N-central and on what build.

TH-2026-W33-03: JetBrains TeamCity Pre-Auth Deserialisation**P1 CRITICAL: CVSS 9.8; KEV due 8 Aug (LAPSED); CI/CD supply chain**

Hypothesis: An unauthenticated attacker reaches the agent polling endpoints of a TeamCity server and delivers a crafted XStream payload that writes and executes a web shell under the web root. Compromise of a build server yields stored credentials and the ability to alter build artefacts, so the consequence is pipeline integrity rather than one host.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Server Software Component: Web Shell), T1552 (Unsecured Credentials), T1195.002 (Supply Chain Compromise: Software Supply Chain).

IOCs: POST requests to /app/agents/v1/register and /app/agents/v1/commands/error; the TeamCity-AgentSessionId header; a following GET to a random hexadecimal file with a .jspws extension under webapps/ROOT. In teamcity-server.log, a ConversionException whose cause is freemarker.template.utility.UndeclaredThrowableException, a path referencing org.apache.commons.collections.keyvalue.TiedMapEntry, and an HsqlException naming a .jspws file. On a patched server a blocked attempt appears as com.thoughtworks.xstream.security.ForbiddenClassException. Proof-of-concept traffic used the user agent Python-urllib/3.10.

Data Sources: TeamCity server and Java logging files, web server access logs, file integrity monitoring on webapps/ROOT, EDR process telemetry for child processes of the TeamCity Java process.

Detection Guidance: Upgrade to 2025.11.7 or 2026.1.3. Search server logs for the exception signatures above, which distinguish a successful attempt from a blocked one, and check webapps/ROOT for .jspws files, noting the published proof-of-concept deletes its own artefact. Because the in-the-wild claim rests solely on the KEV listing with no published victimology, treat the absence of external reporting as absence of information rather than as evidence you were not targeted.

TH-2026-W33-04: Langflow Unauthenticated RCE, 32 Instances Exposed in South Africa**P2 HIGH: CVSS 9.8; default deployments; 650 attempts from 244 IPs since 6 Jul**

Hypothesis: An unauthenticated attacker requests a superuser token from a Langflow instance and then submits Python for execution, achieving remote code execution on a default deployment with no credentials and no user interaction. Langflow instances are frequently stood up by data and AI teams outside normal change control, so the asset may not appear in a patch-management inventory at all.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059.006 (Command and Scripting Interpreter: Python), T1078 (Valid Accounts), T1552 (Unsecured Credentials).

IOCs: POST to /api/v1/auto_login followed by POST to /api/v1/validate/code from the same source address, and any unexpected issuance of a superuser token. A related but distinct earlier Langflow campaign staged payloads from 173.212.205.251 on port 8443 and read .env, .db and /etc/passwd; that address belongs to the earlier CVE and is listed here as related activity, not as an indicator for CVE-2026-9198.

Data Sources: Web server and reverse proxy access logs, application logs, egress netflow, cloud workload telemetry, asset inventory reconciliation against known AI and data science deployments.

Detection Guidance: Upgrade to 1.10.1, for which no workaround exists, and put the instance behind an authenticating reverse proxy or VPN. Search access logs for the two-endpoint sequence back to at least 6 July, when attempt telemetry begins. Then inventory AI tooling specifically: the 32 exposed South African instances are the ones a scanner can see, and the population behind corporate boundaries is likely larger.

TH-2026-W33-05: Apache Tomcat Tribes Clustering on TCP 4000**P2 HIGH:** 776 Tomcat instances exposed in ZA, but port 4000 is the real surface

Hypothesis: The exposed surface is any Tomcat instance whose Tribes cluster receiver on TCP 4000 is reachable by an attacker, with the EncryptInterceptor configured and deserialisation gadget classes present, rather than the web-facing estate as a whole. A crafted message that fails to decrypt is logged and then forwarded into deserialisation regardless, and the payload executes silently.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1210 (Exploitation of Remote Services), T1059 (Command and Scripting Interpreter).

IOCs: A SEVERE log line reading 'EncryptInterceptor.messageReceived Failed to decrypt message' accompanied by javax.crypto.AEADBadTagException Tag mismatch or a BadPaddingException, with no deserialisation error following it. That silence after the error is the tell. Tribes wire framing carries a seven-byte header FLT2002, a four-byte length, the payload, and a seven-byte footer TLF2003.

Data Sources: Tomcat catalina and application logs, host and network firewall rules, internal network scanning results, Kubernetes NetworkPolicy configuration, east-west netflow.

Detection Guidance: Inventory every listener on TCP 4000 and confirm none is reachable from an untrusted network; the port binds to the primary interface rather than localhost and accepts connections without membership verification. Upgrade to 11.0.21, 10.1.54 or 9.0.117. In container platforms check for namespaces without NetworkPolicy, the realistic exposure scenario. Do not treat the national figure as a vulnerable count.

TH-2026-W33-06: Debt Review and Payment Distribution Fraud Following DC Partner**P3 MEDIUM:** no atomic indicators; downstream consequence of a confirmed breach

Hypothesis: Whether or not any dataset is ultimately published, a confirmed breach at a payment distribution agency makes convincing financial social engineering against debt review consumers materially more likely. An approach that quotes a correct outstanding balance, instalment amount and creditor list defeats the verification most consumers and call centre staff actually perform.

MITRE ATT&CK: T1566 (Phishing), T1598 (Phishing for Information), T1656 (Impersonation), T1657 (Financial Theft).

IOCs: None. This mission has no atomic indicators and none should be invented for it. What it has instead are behavioural conditions, listed under detection guidance.

Data Sources: Debit order dispute volumes and reason codes, inbound contact centre call recordings and notes, banking fraud reporting channels, e-mail gateway telemetry for messages referencing debt review or payment distribution, brand monitoring for lookalike domains.

Detection Guidance: For credit providers and debt counsellors: alert on any change to creditor banking details arriving by e-mail, and require out-of-band verification for such changes. Monitor for a rise in debit order disputes originating from PDA-managed accounts. Brief contact centre staff that a caller may quote correct balances and instalment amounts, so knowledge of account detail must stop functioning as proof of identity. For employers: staff under debt review are a population that will not self-identify, so any awareness message has to go to everyone rather than to a list.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. **Close the five overdue KEV items on Tuesday 11 August, in this order:** N-able N-central to Hotfix 2 build 2026.3.1.10, IBM Langflow to 1.10.1, JetBrains TeamCity to 2025.11.7 or 2026.1.3, Apache Tomcat to 11.0.21, 10.1.54 or 9.0.117, and Progress LoadMaster to GA 7.2.63.2 or LTSF 7.2.54.18 before its deadline expires the same day. Order by whether an attacker gains control of other systems: N-central first because it administers customer estates, TeamCity second because it builds and signs software.
2. **Treat SonicWall SMA 1000 as compromised rather than unpatched.** At twenty-four days past its KEV date and with INC Ransomware now the dominant actor on the chain, the appliance requires a rebuild, credential rotation and re-enrolment of multi-factor seeds. A patch applied now does not remove access obtained earlier through stolen session material.
3. **Inventory two things a normal patch cycle will not find:** listeners on TCP 4000 across the Tomcat estate, and Langflow or comparable AI tooling stood up outside change control.
4. **Deploy the Krybit indicators and hunt for exfiltration rather than encryption.** The group takes 10 to 250 GB before encrypting, so bulk outbound transfer is the earlier signal. The 59 indicators in iocs_w33.csv include a sample hash, note and extension artefacts, onions, Tox IDs and Bitcoin wallets.
5. **Ask your managed service provider, in writing, whether they run N-able N-central and what build they are on.** The answer determines whether your estate was reachable through a third party in early August.

Management (CISO / Board)

1. **Use the INTERPOL figure to settle the proportionality question.** South Africa accounts for 92 per cent of African ransomware detections, 70 per cent of business e-mail compromise detections and 43.6 per cent of the vulnerability detections identified by the Shadowserver Foundation. A board treating cyber risk as a global average applied locally now has a sourced reason to treat South African exposure as materially higher than that average.
2. **Reconsider what a supplier assurance question actually asks.** Two of this week's confirmed South African breaches sit at organisations that hold operational data about other companies: payment distribution for creditors and consumers, and physical security for client premises. The useful question to a supplier is not whether they are certified but what data they hold about you and your staff, and what they would tell you and when.
3. **Do not rely on regulatory publication as an early warning channel.** The Information Regulator has published nothing for ten weeks, including the week in which two organisations confirmed breaches and stated they had notified it. Whatever the reason, the practical consequence is that your organisation will not learn about a sector incident from the Regulator in useful time.
4. **Note where the exploited surface moved this quarter.** Since W30 this report has led with perimeter appliances. This week three of six KEV additions were developer and management tooling. Budget and

attention that has been directed at the firewall estate should extend to the build pipeline, the RMM platform and whatever AI tooling has been deployed in the past year.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 13th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for a thirteenth consecutive week (2 August to 8 August 2026). Escalation to CRITICAL was considered more seriously than in any edition since W17 and was still rejected. Two South African organisations confirmed breaches inside the window and one of them is regulated payment infrastructure, which is a materially worse position than a week of unconfirmed claims. Against that: DC Partner reports its systems fully operational and is discharging its POPIA obligations, Fidelity states no third-party or customer data was affected, neither event produced a service disruption at a systemically important institution, and no South African bank, payment scheme or national system has been affected. CRITICAL is reserved for a live national-scale event and this is not one. De-escalation is not supportable while five KEV additions sit past their deadline, two tracked carryovers remain overdue at twenty-four and twenty-three days, managed service provider software is under active exploitation with confirmed downstream reach, and an actor with three South African victims in six days remains active.

Rationale

- **A confirmed breach at regulated payment infrastructure:** DC Partner, one of four NCR accredited payment distribution agencies, confirmed a ransomware attack and is issuing section 22 notifications. The actor claims to have published the data; the scope is unverified.
- **A confirmed breach with data actually published:** Fidelity Services Group confirmed its incident and RansomHouse released a dataset, the first time in this series a South African dataset claimed by an actor has demonstrably been released.
- **One actor, three South African victims in six days,** after a single South African victim in the preceding four months, with a wider African victim cluster visible in the same feed.
- **Two bodies quantified the exposure in the same week:** INTERPOL put South Africa at 92 per cent of African ransomware detections, 70 per cent of business e-mail compromise detections and 43.6 per cent of the vulnerability detections identified by the Shadowserver Foundation, with AI in 55 per cent of African cybercrime cases; SABRIC put digital banking crime losses at R2.4 billion for 2025, up from about R1.9 billion.
- **Five of six KEV additions expired before publication,** and two of the six are the same N-able N-central weakness patched twice, the second entry being an incomplete fix for the first.
- **The overdue backlog deepened:** SonicWall SMA is twenty-four days past its date with a dominant ransomware actor now attached to it, and Oracle E-Business Suite twenty-three.
- **No regulatory signal at all:** the Information Regulator has published nothing since 2 June, ten weeks, including the week two organisations confirmed breaches and said they had notified it.

Next-Week Watch (W34)

- **DC Partner:** whether a dataset actually appears, whether the National Credit Regulator or the Information Regulator responds to a confirmed breach at regulated payment infrastructure, and whether any integrated platform or creditor reports downstream effects.
- **Krybit's African tempo:** whether further African victims are claimed, and whether they cluster in time as 2 August did. The distinguishing test between a deliberate regional campaign and affiliate coincidence is temporal clustering across countries, not the raw count.
- **Fidelity Services Group:** whether the published dataset is analysed by any party, and whether the company's position that no customer data was affected survives that analysis.
- **N-able N-central:** whether the vendor confirms that Hotfix 1 was itself bypassed. The distinguishing observation is any victim reported compromised while running build 2026.3.1.7.
- **JetBrains TeamCity:** whether published victimology appears. The exploitation claim currently rests solely on the KEV listing, and either corroboration or continued silence is informative.
- **Buzz Trading 104 and Serengeti Estates:** corroboration, denial or publication, and whether either follows DC Partner into confirmation.
- **Fastjson CVE-2026-16723:** whether Alibaba patches the 1.x branch, whether CISA adds it to KEV, and whether any confirmed compromise is published as distinct from attempted exploitation.
- **The Information Regulator:** whether anything at all is published in week eleven, particularly on the two breaches notified to it this week.

12. OSINT SOURCES CONSULTED

All sources below are TLP:WHITE and publicly accessible. Numbers correspond to the inline footnotes, assigned in order of first citation, with each unique source appearing once. Every cited URL was directly retrieved and confirmed to contain the claim attributed to it, on 9 August 2026.

Collection notes. An earlier collection on 9 August 2026 was interrupted when the source address was rate limited by one provider, which was established as rate limiting rather than a service outage. The authoritative collection completed at 07:21 UTC on 9 August 2026 and passed its integrity check; all ransomware figures carry that retrieval time, and Shodan figures were retrieved at 07:44 UTC. The 119 record count was corroborated by a separate collection on 8 August using a different endpoint and service tier, which names several fields differently; that difference is now normalised at collection. No Krybit indicators or detection rules were returned by the enrichment endpoint, so Section 9 draws its Krybit indicators from published vendor research instead. Shodan queries were derived from the KEV catalogue for the first time in this edition: Apache Tomcat and Langflow resolved to corroborated fingerprints, JetBrains TeamCity did not and carries no published figure, and N-able N-central and Progress LoadMaster have no usable fingerprint at all.

1. MyBroadband, SA payment distribution agent for FNB and the NCR hit by data breach (7 August 2026). <https://mybroadband.co.za/news/security/661578-south-african-payment-distribution-agent-for-fnb-and-the-national-credit-regulator-hit-by-cyber-attack.html>

2. Ransomware.live, SA victim records via the API victims endpoint, 119 records, purity 1.0 (retrieved 9 August 2026). <https://www.ransomware.live/map/ZA>

3. DC Partner, NCR Registration: number NCRPDA02, one of four registered PDAs in SA (retrieved 9 August 2026). <https://www.dcpartner.co.za/NCR-Registration>
4. Ransomware.live, Victim record: Serengeti Estates / Krybit (discovered 7 August 2026). <https://www.ransomware.live/id/d3d3LnNlcmVuZ2V0aWVzdGF0ZXMuY28uemFAa3J5YmI0>
5. MyBroadband, SA's largest private security company suffers data breach (7 August 2026). <https://mybroadband.co.za/news/security/661700-south-africas-largest-private-security-company-suffers-data-breach.html>
6. INTERPOL, INTERPOL report finds AI linked to more than half of cybercrime in Africa (3 August 2026). <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-finds-AI-linked-to-more-than-half-of-cybercrime-in-Africa>
7. INTERPOL, African Cyberthreat Assessment Report 2026 (released 3 August 2026; 36 member countries). <https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026>
8. Huntress, N-able N-central vulnerability exploitation (3 August 2026). <https://www.huntress.com/blog/n-able-vulnerability-exploitation>
9. Algoa FM, Digital banking crime costs South Africans R2.4bn (7 August 2026; SABRIC 2025 statistics). <https://www.algoafm.co.za/business/digital-banking-crime-costs-south-africans-r2-4bn-as-fraudsters-target-consumers>
10. SOCRadar, Dark web profile: Krybit ransomware. <https://socradar.io/blog/dark-web-profile-krybit-ransomware/>
11. IT-Online, Rectron's doors reopen (27 July 2026). <https://it-online.co.za/2026/07/27/rectrons-doors-reopen/>
12. BlackFog, The State of Ransomware: July 2026 (4 August 2026; CKR and BE Travel entries). <https://www.blackfog.com/the-state-of-ransomware-july-2026/>
13. Halcyon, KryBit threat group profile (RaaS from March 2026; affiliate model; sample hash). <https://www.halcyon.ai/threat-group/krybit>
14. PCrisk, Krybit ransomware analysis (.KRYBIT extension, RECOVER-README.txt). <https://www.pcrisk.com/removal-guides/35210-krybit-ransomware>
15. DeXpose, Krybit ransomware targets DC Partner in South Africa (3 August 2026). <https://www.dexpose.io/krybit-ransomware-targets-dc-partner-in-south-africa/>
16. Halcyon, OAPT vs KryBit: actors list opposing operators as victims (April 2026). <https://www.halcyon.ai/ransomware-research-reports/Oapt-vs-krybit-ransomware-actors-list-opposing-operators-as-victims>
17. N-able, N-central security update (6 August 2026; Hotfix 2 build 2026.3.1.10; attacker IP list). <https://www.n-able.com/blog/n-central-security-update-august-6-2026>
18. The Hacker News, CISA flags Langflow RCE, Tomcat and N-central flaws (August 2026). <https://thehackernews.com/2026/08/cisa-flags-langflow-rce-tomcat-and-n.html>
19. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.07 (retrieved 9 August 2026). <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
20. Rapid7, CVE-2026-18577 N-able N-central auth bypass exploited in the wild (2 August 2026). <https://www.rapid7.com/blog/post/etr-cve-2026-18577-n-able-n-central-authentication-bypass-exploited-in-the-wild/>
21. The Register, N-able confirms attackers reached customer networks as second hotfix lands (7 Aug 2026). <https://www.theregister.com/networks/2026/08/07/n-able-god-mode-flaw-vendor-confirms-attackers-reached-customer-networks-as-second-hotfix-lands/5284730>
22. Striga, Apache Tomcat Tribes unauthenticated RCE, CVE-2026-34486 technical analysis. <https://www.striga.ai/research/tomcat-tribes-unauth-rce>
23. IBM, Security Bulletin: Langflow code injection CVE-2026-9198 (fixed in 1.10.1). <https://www.ibm.com/support/pages/node/7278927>
24. Rapid7, Unauthenticated RCE in JetBrains TeamCity, CVE-2026-63077 (7 August 2026). <https://www.rapid7.com/blog/post/ra-unauthenticated-rce-in-jetbrains-teamcity-cve-2026-63077/>
25. SecurityWeek, Hackers start exploiting recent JetBrains TeamCity vulnerability (August 2026). <https://www.securityweek.com/hackers-start-exploiting-recent-jetbrains-teamcity-vulnerability/>
26. watchTower Labs, Progress Kemp LoadMaster uninitialized heap to pre-auth RCE, CVE-2026-8037. <https://labs.watchtower.com/enterprise-tech-in-shell-out-progress-kemp-loadmaster-uninitialized-heap-to-pre-auth-rce-cve-2026-8037/>
27. eSentire, Progress Kemp LoadMaster targeted, CVE-2026-8037 (attempts from 29 June 2026). <https://www.esentire.com/security-advisories/progress-kemp-loadmaster-vulnerability-targeted-cve-2026-8037>
28. The Hacker News, INC Ransomware emerges as dominant actor on the SonicWall SMA chain (August 2026). <https://thehackernews.com/2026/08/inc-ransomware-emerges-as-dominant.html>
29. Shodan host/count exposure queries for South Africa, VERIFIED fingerprints only (9 August 2026). <https://www.shodan.io/>
30. Information Regulator (SA), Media statements index; most recent statement 2 June 2026 (checked 9 August 2026). <https://infoeregulator.org.za/media-statements/>
31. FIRST, South African CSIRT directory: six teams (retrieved 9 August 2026). <https://www.first.org/members/teams/>

Classified TLP:WHITE and distributable without restriction. Sourced from publicly available OSINT; no classified or restricted sources were used. Single-source and threat-actor claims are rated PROBABLE or CLAIMED in the text. SA-CTI-2026-W33 | Published Monday 10 August 2026