



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 34 | 9 August – 15 August 2026

THREAT LEVEL: HIGH

TLP:WHITE

Report ID: SA-CTI-2026-W34 | Classification: TLP:WHITE

Published Monday 17 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 (W34)**
- 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@orange cyberdefense.com

R20 500
PER COURSE

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH, 17th consecutive week (9 August - 15 August 2026)

Story 1. LEGO Certified Stores South Africa issued a section 22 notification on 14 August 2026 telling customers that their email addresses and mobile telephone numbers had been accessed.^{1,2} Nobody broke into the shop. The flaw was in a product two companies further down the chain: from the retailer, to Marsello as the POPIA operator running its loyalty programme, to Metabase, a reporting tool Marsello uses internally; none of the three companies' own applications was breached. Exploitation was on 5 August, Metabase fixed it on 6 August, Marsello applied the fix immediately and confirmed the loss to the retailer on 14 August.^{1,3} A one-day patch cycle is faster than most South African organisations manage and the data went anyway, because exploitation preceded disclosure. The flaw is CVE-2026-72898, an unauthenticated SQL injection with an NVD base score of 10.0, in KEV from 11 August and due 14 August.^{4,5,6} There are 84 Metabase instances exposed in South Africa.⁷ First reported by [MyBroadband](#) on 14 August 2026.

Story 2. LEGO Certified Stores was one of three South African organisations to confirm an incident this week, and all three sit on the supply chain, though not in the same place on it. The other two follow. Toyota South Africa Motors confirmed customer personal information may have been exposed through a third-party bulk SMS provider, after that provider's account was used to push fraudulent messages advertising a gambling promotion the carmaker never authorised.⁸ Euphoria Telecom confirmed unauthorised access to its cloud environment on 16 July 2026, restricted international dialling against potentially exposed SIP credentials, rotated them, and reported the matter to the Information Regulator.⁹ Euphoria is the third case and the different one: the compromise was of its own environment, and it matters here because Euphoria is itself a supplier, holding the telephony credentials of the South African businesses that buy from it. No ransomware group listed a South African victim inside the window. Toyota first reported by [MyBroadband](#) on 14 August 2026; Euphoria first reported by [MyBroadband](#) on 13 August 2026.

Story 3. The most quoted South African cyber statistic of the past fortnight belongs to a security vendor rather than to INTERPOL, and this report helped spread it without saying so. INTERPOL's African Cyberthreat Assessment Report 2026 states that South Africa accounted for 92 per cent of all ransomware detections in Africa by TrendAI, its Figure 4 captioned "Ransomware detections by country in 2025 (Source: TrendAI)".¹⁰ W33 attributed it to INTERPOL alone. A detection share measures where a vendor has sensors. Cabo Verde ranks second at 4 per cent, which describes an install base rather than a ransomware problem.¹⁰ South African coverage carried the figure without the vendor attribution.^{11,12} First reported by [IOL](#) on 4 August 2026. The full correction is below.

Corrections to Prior Editions

Three corrections are owed. The first changes a figure printed on the cover of every edition since W21.

- **Correction 1, to W21 through W33: the consecutive-week counter was wrong by three.** The rolling metrics file records the threat level as HIGH without interruption from W18 onward, W17 having been

the only CRITICAL week of 2026. That is sixteen consecutive HIGH weeks to W33 and seventeen to W34. W32 printed a twelfth week and W33 a thirteenth. The error was inherited forward without anyone recounting against the underlying record, was identified in the W33 independent review, and was held over because changing a cover figure needed an explicit decision. Every reference in this edition reads seventeenth; readers holding earlier PDFs should add three to any streak figure from W21 onward.

- **Correction 2, to W33: the INTERPOL ransomware figure is TrendAI telemetry.** W33 reported that INTERPOL put South Africa at 92 per cent of African ransomware detections, and treated the 70 per cent business email compromise figure the same way, while correctly naming the Shadowserver Foundation for the 43.6 per cent vulnerability figure. The report's own wording is "South Africa accounted for 92 per cent of all ransomware detections in Africa by TrendAI", and Figure 4 is captioned "Ransomware detections by country in 2025 (Source: TrendAI)". The denominator is one vendor's detection telemetry for calendar 2025. It is neither an INTERPOL incident count nor a measure of how much ransomware South Africa suffers, and the distribution shows why: South Africa 92 per cent, Cabo Verde 4 per cent, then Kenya, Madagascar, Nigeria and all other countries at 1 per cent each. Leak-site counts put South Africa at roughly a fifth to a quarter of African listings, consistent with this report's own feed. For completeness on what the survey does source: the 55 per cent AI figure and the 89 per cent underreporting figure come from INTERPOL's member-country survey, not from detection telemetry.^{10,13}
- **Correction 3, to W32 and W33: Alibaba Fastjson 1.x is patched, and already was when W33 said it was not.** The W33 tracking table recorded CVE-2026-16723 as "still unpatched on 1.x" and W32 carried the same characterisation. Alibaba published fastjson 1.2.84 on 29 July 2026 and archived the repository the same day. The error survived because the vendor's own advisory page was last edited on 21 July and still directs readers to safe mode or a fastjson2 migration without mentioning the release. Move to 1.2.84 or later, or to fastjson2. Details are in Section 5.^{14,15}

KPI Dashboard

Metric	Current (W34)	Prior (W33)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (17th week)	FLAT
ransomware.live SA cumulative	119	119	0	FLAT
SA claims dated inside the window	0	3	-3	DOWN
SA breaches confirmed by the victim	3	2	+1	UP
New CISA KEV additions	3	6	-3	DOWN
KEV adds already overdue at publication	2	5	-3	DOWN
KEV adds with a VERIFIED SA exposure figure	1 of 3	2 of 6	-1	DOWN
Corrections issued to prior editions	3	4	-1	DOWN
Weeks since last IR publication	11	10	+1	UP

W34 KEY FRAMING: every South African incident confirmed this week sits on a supply chain, and the week shows both ends of one. Two organisations were reached through their suppliers, a marketing operator's internal reporting tool and a bulk SMS platform. The third, Euphoria Telecom, was compromised directly, and it is a supplier: it holds the telephony credentials of the South African businesses that buy cloud PBX from it, which is why it restricted their international dialling before it restored it. No ransomware group listed a South African victim at all. The board question is not whether your own patching is adequate, because in the LEGO chain the patch was applied within a day and the data was gone before it existed. It is which of your suppliers holds your customer data, what they run it on, and how quickly they are contractually obliged to tell you. For SOC readers the technical centre of the week is the credential concentrator: a business intelligence tool holds standing connections to every database it reports on, so an administrative compromise of the reporting layer reaches data that layer was never meant to expose. Metabase's own guidance is to rotate the credentials for every connected database, and that is the step teams skip.

TOP 3 ACTIONS THIS WEEK

1. Patch self-hosted Metabase on Monday 17 August, then assume compromise and rotate every connected database credential. Fixed builds are 63.5, 62.9, 61.11, 60.17, 59.21 and 58.24; where patching is not possible immediately, block the /api/session/reset_password endpoint at the proxy. Then run the vendor's own compromise check: a POST to /api/session/reset_password returning 400, followed by a GET to /api/user/current returning 200, in application or ingress logs. If that pattern is present, delete all rows in the core_session table to revoke active sessions, audit API keys and administrator accounts, and rotate the credentials for every database the instance connects to. Public proof-of-concept exploits were open sourced from 10 August, so the window in which only the original operator could exploit this has closed.

2. Ask your three largest data-handling suppliers, in writing this week, what they run your customer data on and when they will tell you. Two of the three South African incidents confirmed this week reached the victim through an operator or platform, and the third happened at a supplier. Put three questions: which sub-processors and internal tools touch our records, what is your notification deadline to us in hours rather than the phrase without undue delay, and will you tell us about an incident at your own supplier. POPIA makes the responsible party accountable for an operator's processing, so the regulatory exposure sits with you regardless of where the flaw was.

3. Apply the Cisco ASA and FTD fix, and treat any Metabase or N-central instance left unpatched in the first fortnight of August as compromised rather than exposed. CVE-2026-20349 entered KEV on 11 August due 14 August, overdue by three at publication: a remote unauthenticated denial of service against the firewall itself. No South African figure is published for it, because the catalogue product string has no Shodan fingerprint; the 357 ASA WebVPN portals counted in Section 7.2 are a different query and do not stand in for it. On N-central, the vendor's own wording is that Hotfix 2 closes the way in but does not remove an actor already present, and that an environment hotfixed more than a few days late should be treated as potentially compromised. Microsoft attributes the ransomware activity to Storm-1175, which has moved from Medusa to a new strain called StormEncryptor, and assesses the intrusion likely involves CVE-2026-18577.

1. LEGO Certified Stores South Africa, section 22 POPIA data breach notification to affected customers (14 August 2026). Received primary document, not published online.

2. MyBroadband, Lego Certified Stores South Africa hit by zero-day hack of third-party database provider (14 August 2026). <https://mybroadband.co.za/news/security/662655-lego-certified-stores-south-africa-hit-by-zero-day-hack-of-third-party-database-provider.html>

4. The Hacker News, Metabase Zero-Day Exploited in Wild Allows Admin Access Without Authentication (8 August 2026, updated 11 August). <https://thehackernews.com/2026/08/metabase-zero-day-exploited-in-wild.html>

5. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.14, released 14 August 2026, retrieved 16 August 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

6. NVD CVSS base scores with scoring source, retrieved 16 August 2026. <https://nvd.nist.gov/>

7. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 16 August 2026. <https://www.shodan.io/>

8. MyBroadband, South African Toyota customers' personal info possibly leaked after SMS provider breach (14 August 2026). <https://mybroadband.co.za/news/security/662372-south-african-toyota-customers-personal-info-possibly-leaked-after-sms-provider-breach.html>

9. MyBroadband, Euphoria Telecom contains breach after it suffers cyberattack (13 August 2026). <https://mybroadband.co.za/news/security/662245-euphoria-telecom-contains-breach-after-it-suffers-cyberattack.html>

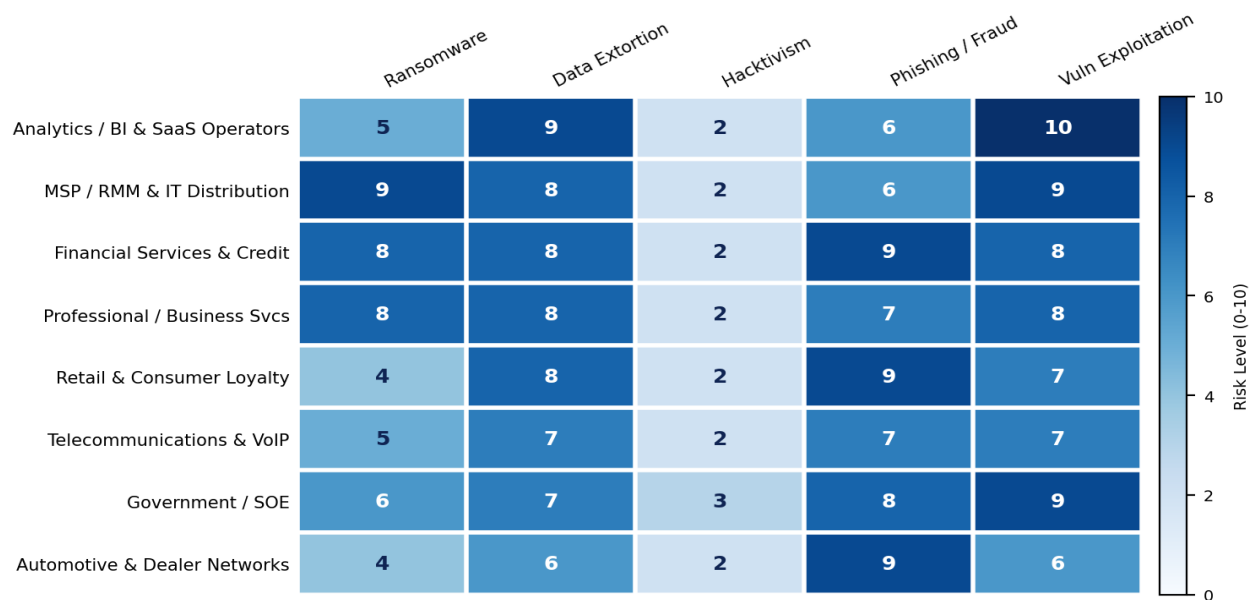
10. INTERPOL, African Cyberthreat Assessment Report 2026, released 3 August 2026, PDF cover dated June 2026. Figure 4, Ransomware detections by country in 2025, Source: TrendAI. <https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026>

11. IOL, South Africa named Africa's cybercrime hotspot (4 August 2026). <https://iol.co.za/news/crime-and-courts/2026-08-04-south-africa-named-africas-cybercrime-hotspot/>

16. Wiz Research, Inside the Metabase SQLi: Exploited in the Wild (10 August 2026).
<https://www.wiz.io/blog/inside-the-metabase-sqli-exploited-in-the-wild>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W34 (9 - 15 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, and the four that enter are the sectors that produced this week's confirmed incidents. **Analytics, BI and SaaS Operators, Retail and Consumer Loyalty, Telecommunications and VoIP** and **Automotive and Dealer Networks** enter, replacing Security and Facilities Services, Manufacturing and Wholesale, Property and Hospitality, and Healthcare and Medical Schemes. Analytics, BI and SaaS Operators enters at 10 on Vulnerability Exploitation, on the strength of CVE-2026-72898: NVD base score 10.0, exploited as a zero-day before disclosure, public proof-of-concept code, and 84 instances exposed in South Africa.^{5,16,7,6} It enters at 9 on Data Extortion and only 5 on Ransomware, because the outcome across every published victim of this campaign has been data theft rather than encryption. Retail and Consumer Loyalty and Automotive and Dealer Networks both enter at 9 on Phishing and Fraud rather than on Ransomware, because the harm described is brand-impersonation phishing and smishing against people whose contact details now sit alongside a known brand name, and the Toyota incident has already produced fraudulent messages sent from a legitimate sender identity.^{1,8}

Two retained rows also move, and neither reflects an improvement in posture. Financial Services and Credit steps down from 9 to 8 on both Ransomware and Data Extortion, and Professional and Business Services does the same, in each case because no new listing appeared in those sectors this week while DC Partner and CKR Consulting Engineers remain open in Section 3. MSP, RMM and IT Distribution holds at 9

on both Ransomware and Vulnerability Exploitation, because N-central exploitation continued through the window with new victim reporting and a probable actor attribution.^{17,18} Government and SOE is unchanged. Retiring Security and Facilities Services does not close the Fidelity Services Group matter, which stays in the carryover list.

3. TOP SA INCIDENTS (W34)

Week 34 recorded no South African leak-site listing dated inside the window and three South African organisations that confirmed security incidents in their own words. Two were reached through a supplier; the third was compromised directly and is itself a supplier to other South African businesses. They are set out below in order of how far the compromise sat from the organisation whose customers were affected.

3.1 INC-2026-W34-01: LEGO Certified Stores South Africa, Fourth-Party Breach via Metabase [CONFIRMED]

Sector	Retail and consumer loyalty
Responsible party	LEGO Certified Stores South Africa, the local franchise operator
Operator	Marsello, which runs the customer loyalty and marketing programme
Fourth party	Metabase, a business intelligence tool used internally by Marsello
Timeline	Exploited 5 August 2026. Vendor fix 6 August, applied by Marsello immediately. Confirmed to the responsible party 14 August
Data affected	Email addresses and mobile telephone numbers. No banking, payment or card data, no account passwords. Numbers affected not stated
Vulnerability	CVE-2026-72898, unauthenticated SQL injection, NVD base score 10.0
Regulator	Not stated in the customer notice
Confidence	CONFIRMED. Statutory section 22 notice issued by the responsible party, corroborated by national technology press

On 14 August 2026 LEGO Certified Stores South Africa issued a notification under section 22(1)(b) of the Protection of Personal Information Act to affected customers, reported by MyBroadband the same day.^{1,2} The notice states that an unauthorised third party exploited a previously unknown vulnerability in Metabase on 5 August 2026, that Metabase notified Marsello and released a fix on 6 August, which the vendor advisory independently dates to the same day,³ and that Marsello applied it immediately, then identified unusual activity, investigated, and confirmed on 14 August that the vulnerability had been used to access customer contact information. Neither its own systems nor the Marsello application itself were compromised, and access was limited to information held within the reporting tool.^{1,2} This report works from the section 22 notice received directly; the incident was first reported publicly by MyBroadband on 14 August 2026.

The structure is what makes this worth a board's attention. A customer transacted with a toy retailer; their contact details sat with that retailer's marketing operator and were read out of a reporting tool the operator uses internally. Three organisations sit between the customer and the flaw and none had a vulnerability in the product they sell. Under POPIA the responsible party stays accountable for processing carried out by an operator, so the obligation landed on the retailer regardless of where in the chain the defect sat.

The timeline deserves reading by anyone who believes patching speed is a strategy. Exploitation on 5 August, vendor fix on 6 August, applied immediately. That is a one-day cycle, faster than the great majority of South African organisations achieve, and the data was taken anyway because the attacker was using the flaw before the vendor knew it existed. Nine days then passed between exploitation and the data subject being told, which measures how long a fourth-party incident takes to surface rather than criticising the retailer, which notified promptly once Marsello confirmed.

As at 16 August no Marsello statement had been located and no other South African brand identified as notifying over the same incident, which given Marsello's retail customer base is a live question.

Detection relevance: TH-2026-W34-01 carries the vendor's compromise signature and the credential rotation that follows it; TH-2026-W34-03 covers which business intelligence tools in your own estate hold standing database connections; TH-2026-W34-07 covers the brand-impersonation phishing the notice itself predicts.

1. LEGO Certified Stores South Africa, section 22 POPIA data breach notification to affected customers (14 August 2026). Received primary document, not published online.

2. MyBroadband, Lego Certified Stores South Africa hit by zero-day hack of third-party database provider (14 August 2026). <https://mybroadband.co.za/news/security/662655-lego-certified-stores-south-africa-hit-by-zero-day-hack-of-third-party-database-provider.html>

3. SecurityWeek, Metabase Patches Vulnerability Exploited as Zero-Day (10 August 2026), quoting the vendor advisory GHSA-vwf4-m7j8-wcjf. <https://www.securityweek.com/metabase-patches-vulnerability-exploited-as-zero-day/>

11. IOL, South Africa named Africa's cybercrime hotspot (4 August 2026). <https://iol.co.za/news/crime-and-courts/2026-08-04-south-africa-named-africas-cybercrime-hotspot/>

3.2 INC-2026-W34-02: Toyota South Africa Motors, Third-Party SMS Platform Abuse [CONFIRMED]

Sector	Automotive and dealer networks
Responsible party	Toyota South Africa Motors
Third party	A bulk SMS services provider, not named
Notification	Customers first notified late July 2026 by SMS and website notice; detailed reporting 12 and 14 August 2026
Effect	Unauthorised distribution of fraudulent SMS messages promoting a purported gambling collaboration
Data affected	Customer personal information that "may have been exposed". Scope not quantified
Regulator	TSAM states relevant authorities and regulators were engaged
Confidence	CONFIRMED as an incident by the company. The extent of personal-information exposure remains the company's own qualified statement

Toyota South Africa Motors confirmed that customers whose personal information may have been exposed in an incident at a third-party SMS services provider have been notified, having begun notifying in late July 2026 by SMS and a website notice. The provider's account was used to send fraudulent messages promoting a purported gambling collaboration that the carmaker says it never authorised, endorsed or initiated. TSAM activated incident response procedures, engaged the provider, and locked the affected account while the investigation continues.⁸ First reported by [MyBroadband](#) on 14 August 2026.

The mechanism matters more than the volume. South African businesses routinely use third-party bulk SMS platforms, which send from a registered sender identity recipients have been trained to trust, and an attacker with access to that account inherits the trust wholesale. Every control a consumer has been taught to apply fails, because the message did come from the right sender. This is the failure mode SARS described in its 28 July alert about AI-generated phishing quality, by a different route.

Two elements remain unresolved. The SMS provider has not been named, which is a material gap for any other South African brand trying to establish whether it shares that supplier, and the gambling entity referenced in the messages is unclear.⁸ This report names neither as a participant.

Detection relevance: TH-2026-W34-05 covers bulk SMS platform account abuse, including the telemetry a marketing team holds and a security team usually does not.

7. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 16 August 2026. <https://www.shodan.io/>

3.3 INC-2026-W34-03: Euphoria Telecom, Unauthorised Cloud Access and SIP Credential Exposure [CONFIRMED]

Sector	Telecommunications and cloud telephony
Organisation	Euphoria Telecom, a South African cloud PBX and contact-centre provider
Timeline	Detected 16 July 2026. Public 13 August 2026, after a customer tip-off to the press
Nature	Unauthorised access to the cloud environment. Explicitly not ransomware. Risk identified was potentially exposed SIP credentials usable for fraudulent international calls
Containment	Access contained on detection; international dialling restricted; SIP and extension credentials rotated; new fraud-prevention controls
Regulator	Information Regulator notified, and customers notified, under POPIA
Confidence	CONFIRMED. On-record statements by the managing director

Euphoria Telecom confirmed that it detected unauthorised access to its cloud environment on 16 July 2026. Managing director Warren Hawkins said the access was contained on detection and that the company applied precautionary limits on international dialling, because "There was a risk that potentially exposed SIP credentials could be used to make fraudulent international calls." International calling has since been restored as SIP and extension credentials were rotated and new fraud-prevention controls came online. Hawkins said the company reported the matter to the Information Regulator and notified customers in line with POPIA.⁹ First reported by [MyBroadband](#) on 13 August 2026.

Two distinctions are worth preserving. This was not ransomware; Hawkins described an actor gaining unauthorised access to internal data and computer resources. And the credential exposure is stated as a risk rather than a confirmed loss, the company's own word being "potentially", so this report does not record those credentials as stolen. What is confirmed is that the company judged the risk serious enough to degrade its own service by cutting international dialling.⁹

Telephony fraud is the exposure here and it is poorly understood outside telecoms. Compromised SIP credentials are used to place high volumes of calls to premium-rate international destinations the fraudster controls or shares revenue with, typically overnight or over a weekend, and the bill lands on the account holder. The loss is realised in hours and, unlike a data breach, it is immediately financial. Restricting international dialling first and restoring it as credentials rotated is the correct order of operations.

Detection relevance: TH-2026-W34-06 covers SIP credential abuse and toll fraud, which call detail records reveal before any other source does.

8. MyBroadband, South African Toyota customers' personal info possibly leaked after SMS provider breach (14 August 2026). <https://mybroadband.co.za/news/security/662372-south-african-toyota-customers-personal-info-possibly-leaked-after-sms-provider-breach.html>

Carryover Status (checked 16 August 2026)

- **DC Partner (Pty) Ltd and Krybit: OPEN, no change.** The confirmed breach at one of four National Credit Regulator accredited payment distribution agencies produced no development between 9 and 15 August. No dataset has been located or analysed, and neither the National Credit Regulator nor the Information Regulator has published anything.¹⁹ The company's own site confirms the NCR registration and its George address.²⁰ The confirmation was [first reported by MyBroadband](#) on 7 August 2026. Note a date correction to W33's own narrative: the Krybit listing is dated 2 August 2026 at 14:25 UTC, while 7 August is the date of the company's confirmation to the press.
- **Fidelity Services Group and RansomHouse: OPEN, no change.** No published analysis of the released dataset appeared in the window, and the company's position that no third-party or customer information was breached is unchanged, as [first reported by MyBroadband](#) on 7 August 2026.²¹ That position and the actor's publication of data remain irreconcilable from open sources, and both are recorded rather than resolved.
- **Serengeti Estates, Buzz Trading 104, Rectron, Isegen and BE Travel: OPEN, no change.** Neither Krybit listing has been acknowledged, denied or corroborated, and nothing has been observed about the other three since 9 August.²² All five are held as one line because none produced evidence this week.
- **JetBrains TeamCity and Progress LoadMaster: both still short of a confirmed victim.** The TeamCity in-the-wild claim continues to rest on the KEV listing and the vendor's general wording of active and attempted exploitation, with no actor, scale or named victim published.²³ LoadMaster remains listed by CISA on 7 August following reports of active exploitation, but with no publicly confirmed compromise of any named organisation, and the most recent recorded exploitation activity predates this window.²⁴

19. MyBroadband, One of four payment agents accredited by the National Credit Regulator suffers 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>

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

22. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 119 records at filter purity 1.0, retrieved 05:00 UTC on 16 August 2026. <https://www.ransomware.live/>

23. JetBrains, CVE-2026-63077 update (7 August 2026). <https://blog.jetbrains.com/teamcity/2026/08/cve-2026-63077-update/>

24. The Hacker News, Progress Kemp LoadMaster flaw hits CISA KEV catalogue (8 August 2026). <https://thehackernews.com/2026/08/progress-kemp-loadmaster-flaw-hits-cisa.html>

4. THREAT ACTORS

4.1 The Metabase Zero-Day Operator: Unattributed, Multi-Victim, Fast

No vendor or law enforcement body has attributed the Metabase campaign to a named group, and this report does not offer one. What is available is a behavioural profile from the victims' own disclosures, unusually clear because the victims are technology companies that publish detail. Metabase identified the attack against Metabase Cloud and disclosed on 6 August 2026, describing a zero-day in versions 1.58 and above.⁴ Disclosures followed from Framework and Tally on 7 August, n8n on 8 August, Kilo Code on 9 August and ChecklyHQ on 10 August.¹⁶

Three characteristics stand out. The operator moved quickly and in bounded windows: Kilo Code states the incident affecting it "occurred over a period of approximately 4 hours on August 2, 2026", and that it was alerted four days later. The targeting was data rather than disruption: across every published victim the outcome was theft of stored records, with n8n reporting 136 customer records of which five held bcrypt-hashed passwords, Kilo Code reporting exposure of Slack access tokens, and Framework telling customers that names, login IP addresses, addresses, phone numbers and emails were accessed with no order or payment information involved. And the operator understood what a business intelligence tool is for.⁴

The South African consequence, so far as is known, is the LEGO Certified Stores contact data, which is the least severe outcome on the published list and should not be read as a ceiling. Wiz reverse engineered the flaw from the patch on 10 August and observed public proof-of-concept exploits open sourced by noon UTC the same day.¹⁶ Any assessment of who can exploit this changed on that date. First reported by [Wiz Research](#) on 10 August 2026.

4.2 Storm-1175 and N-able N-central: A Named Actor and a New Encryptor

The N-able N-central intrusions gained a named actor during the window. Microsoft attributes the ransomware activity to Storm-1175, a group that has moved from deploying Medusa to a new strain reported as StormEncryptor.¹⁸ Microsoft does not hedge the actor; what it qualifies is the entry point, saying the campaign likely involves exploitation of CVE-2026-18577. Post-compromise tooling reported alongside it includes AnyDesk and SimpleHelp for persistence, Advanced IP Scanner for discovery, and Mimikatz for credential dumping from LSASS.¹⁸

Two independent responders described hands-on behaviour in the same period. Sophos reported domain administrator password resets, a created domain account named "veeam", additional remote-access tooling and the disabling of Microsoft and Sophos protection; Huntress detected exploitation at a

customer, with the actor targeting domain controllers and moving quickly across hosts, and characterised it as targeting the flaw across multiple organisations rather than as a broad campaign.¹⁸ The account name is worth noting: "veeam" in a domain running Veeam backup software survives a cursory review, and backup-adjacent identities are what an actor wants before an encryption event. Full indicators are in TH-2026-W34-02. First reported by [Help Net Security](#) on 10 August 2026.

On the question W33 left open, whether the first hotfix was itself bypassed, N-able has not said. Its position is that Hotfix 2, build 2026.3.1.10 released 6 August, closes "a related attack path" found through continued monitoring. That is compatible with a bypass and with an independently discovered second path, and the vendor has not distinguished them; the observation that would settle it remains a victim compromised while running build 2026.3.1.7, and none has been reported. The operationally important line is unambiguous: "Applying Hotfix 2 closes the vulnerability that allowed attackers in, but it does not remove a threat actor who may already be present. If you applied either hotfix more than a few days after it was released, you should treat your environment as potentially compromised."¹⁷

17. N-able, N-central Security Update, August 10 2026 (published 9 August 2026).

<https://www.n-able.com/blog/n-central-security-update-august-10-2026>

18. Help Net Security, CVE-2026-18577: N-central Hotfix 2 and what MSPs must do now (10 August 2026).

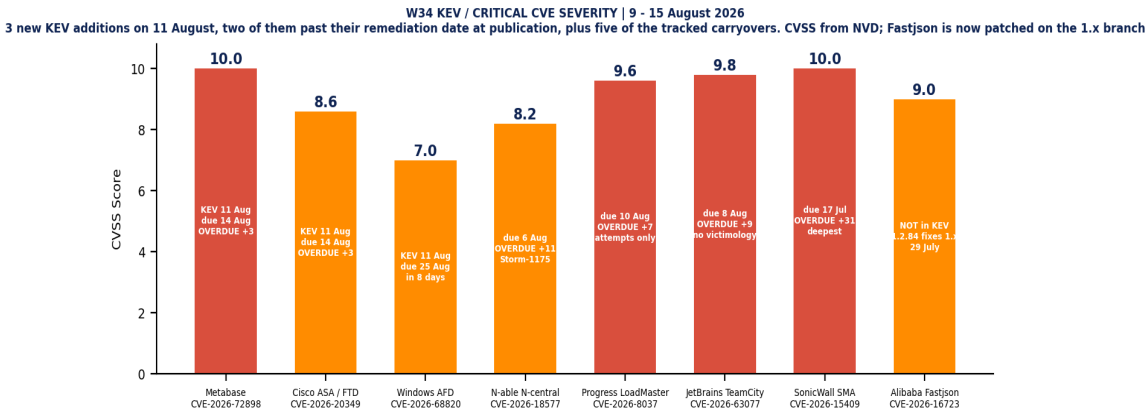
<https://www.helpnetsecurity.com/2026/08/10/cve-2026-18577-n-central-hotfix-2-msps/>

5. CRITICAL VULNERABILITIES & CISA KEV

Three vulnerabilities entered the CISA KEV catalogue in the reporting window, all of them on 11 August 2026, against six the week before.⁵ Two carried a three-day remediation deadline of 14 August and were therefore overdue by three days when this report was published on Monday 17 August; the third carries a 25 August date. Due dates are per entry rather than a uniform interval, and the required action now cites CISA Binding Operational Directive 26-04 rather than the older 22-01.⁵ All CVSS values below are NVD base scores with the scoring source recorded, and all three additions carry a knownRansomwareCampaignUse value of Unknown, which the catalogue distinguishes from no.^{5,6}

Metabase, CVE-2026-72898 is the week's significant entry: an unauthenticated SQL injection at POST /api/session/reset_password, scored 10.0 by NVD under CVSS 4.0, giving administrator access to the instance and, in the vendor's own words, the ability to change configuration, steal stored credentials for connected databases, read anything reachable through those connections and export data.^{4,5,6} Wiz reverse engineered it from the shipped patch: an undocumented user-id key in the JSON body survives a Clojure merge when authentication fails, keywordisation turns the payload into a Clojure map, and HoneySQL's raw directive embeds the attacker's string as unparameterised SQL. The defect entered in version 1.58 with the authentication identity refactor.¹⁶ **Cisco Secure Firewall ASA and FTD, CVE-2026-20349** is a heap inspection weakness, CWE-244, scored 8.6 with availability the only impacted metric: it gives an attacker neither data nor a foothold, it takes the firewall down, which for an organisation whose remote workforce terminates on an ASA is an outage of every remote worker at a time of the attacker's choosing. **Microsoft Windows Ancillary Function Driver for WinSock, CVE-2026-68820** is a use-after-free, CWE-416, scored 7.0, allowing local privilege escalation; a second-stage capability that converts any of the footholds described elsewhere in this edition into SYSTEM, its fourteen-day due date rather than three being the catalogue's own signal about urgency.^{5,6} EPSS for the three is 0.104, 0.0087 and 0.0033.²⁵

W34 CVSS Severity Distribution



W34 CISA KEV / Critical CVE Tracking (new adds 11 August plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-72898	Metabase	10.0	SQL injection (unauth)	14 Aug	KEV 11 Aug. OVERDUE +3. Zero-day before 5 Aug; public PoC from 10 Aug. Fixed 63.5 / 62.9 / 61.11 / 60.17 / 59.21 / 58.24. 84 exposed in ZA. Ransomware: Unknown. EPSS 0.1040.
CVE-2026-20349	Cisco Secure Firewall ASA and FTD	8.6	Heap inspection (unauth DoS)	14 Aug	KEV 11 Aug. OVERDUE +3. Unauthenticated remote reload. Availability only. No Shodan product label exists for this string, so no ZA figure is published. Ransomware: Unknown. EPSS 0.0087.
CVE-2026-68820	Microsoft Windows AFD for WinSock	7.0	Use-after-free (local EoP)	25 Aug	KEV 11 Aug. Eight days to run. Local vector, needs existing access. Converts a foothold to SYSTEM. Ransomware: Unknown. EPSS 0.0033.
CVE-2026-18577	N-able N-central	8.2	Auth bypass	6 Aug	OVERDUE +11. Incomplete patch for CVE-2026-18556. Hotfix 2 build 2026.3.1.10 required. Vendor states hotfixing does not evict an actor already present. Microsoft attributes the activity to Storm-1175; it is the CVE linkage it qualifies.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-18556	N-able N-central	8.2	Auth bypass	7 Aug	OVERDUE +10. Exploited from 1 Aug. Sophos and Huntress both reported hands-on intrusions this window.
CVE-2026-63077	JetBrains TeamCity	9.8	Deserialisation (unauth RCE)	8 Aug	OVERDUE +9. Still no published victimology. Fixed 2025.11.7 / 2026.1.3. EPSS 0.1072.
CVE-2026-8037	Progress LoadMaster	9.6	Command injection (pre-auth)	10 Aug	OVERDUE +7. KEV-listed for active exploitation; no publicly confirmed compromise of a named organisation. Fixed GA 7.2.63.2 / LTSF 7.2.54.18. EPSS 0.9931, highest here.
CVE-2026-34486	Apache Tomcat	7.5	Missing encryption (fail-open)	7 Aug	OVERDUE +10. Reachable via Tribes clustering on TCP 4000 rather than the web port. Fixed 11.0.21 / 10.1.54 / 9.0.117. 836 exposed in ZA, which is an exposure count. EPSS 0.8293.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	OVERDUE +31, the deepest carryover tracked. Credentials, sessions and TOTP seeds are stolen on this chain, so rebuild rather than patch.
CVE-2026-46817	Oracle E-Business Suite	n/a	Improper privilege mgmt	18 Jul	OVERDUE +30. NVD gives 9.8; the KEV catalogue carries no CVSS.
CVE-2026-16723	Alibaba Fastjson 1.x	9.0	Unauth RCE (deserialisation)	n/a	NOT in KEV. CORRECTED THIS WEEK: the 1.x branch IS patched. Release 1.2.84, 29 July 2026, repo archived same day. Move to 1.2.84+ or fastjson2. No confirmed victim.

Pattern note: the overdue column is where this week's finding sits. Three additions is quiet by 2026 standards, but nine tracked items sit past their remediation date and the deepest is thirty-one days old. Two of the three new entries had expired before this report reached a reader, a function of a three-day federal deadline landing on a Friday, and a South African organisation is not bound by that deadline in any case. A lapsed KEV date is best read as a statement that exploitation is real and remediation is not optional, rather than as a compliance clock. On EPSS: LoadMaster scores 0.9931 with no confirmed compromise anywhere, while the Cisco ASA entry scores 0.0087 while listed as exploited. EPSS predicts the next thirty days and lags confirmed activity, so it earns its place ranking items not yet in KEV and must never deprioritise one that is.

14. Alibaba, fastjson release 1.2.84 (29 July 2026). Repository archived the same day.

<https://github.com/alibaba/fastjson/releases/tag/1.2.84>

15. Alibaba, Security Advisory: Remote Code Execution in fastjson 1.2.68 to 1.2.83, last edited 21 July 2026.

<https://github.com/alibaba/fastjson2/wiki/Security-Advisory:-Remote-Code-Execution-in-fastjson-1.2.68%E2%80%931.2.83>

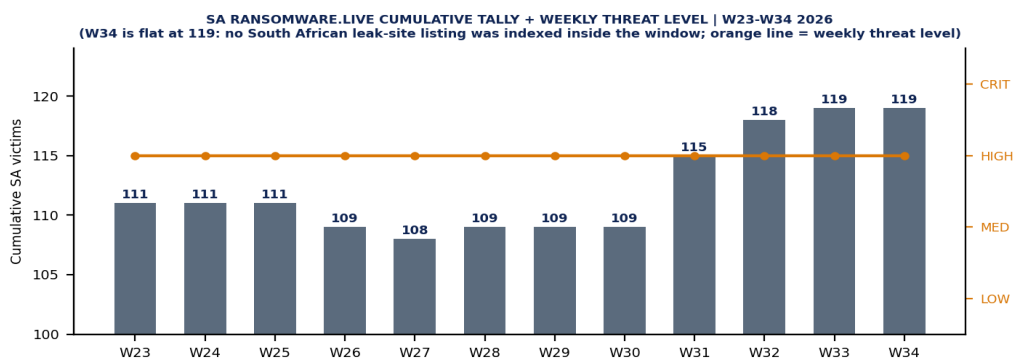
25. FIRST, Exploit Prediction Scoring System scores, retrieved 16 August 2026. <https://www.first.org/epss/>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 119 records when retrieved at 05:00 UTC on 16 August 2026, the same figure as the previous week.²² No South African organisation was listed by any ransomware or extortion group with a discovery date inside the window of 9 to 15 August. The flat total is not a delisting offset by a new listing, and it is not a back-fill: the three most recent South African records are Serengeti Estates on 7 August, DC Partner on 2 August and Buzz Trading 104 on 2 August, all reported in W33, and nothing has been indexed since.²²

Two integrity notes belong with that zero, because an absence is the observation most easily produced by a broken query. The collection passed its checks: the feed is country-scoped by path, returned 119 records of which 119 were South African, and exited clean.²² And the window now closes on Saturday midnight while collection runs at 05:00 UTC on Sunday, a margin that exists because W32 reported a zero that was wrong. This zero was collected the corrected way.

One discrepancy is recorded without a conclusion. The aggregator's public South African map page showed 105 victims on 16 August against 119 from the API the same morning. This report uses the API figure, the authoritative feed with a per-record purity check. Prior editions asserted a cause for a similar discrepancy and were wrong both times they committed, so the distinguishing test is set out in Next-Week Watch rather than a cause being named here.



Baseline at W33 close	119 cumulative South African records
Movement in window	0 new listings, 0 delistings or restorations observed
End count	119, retrieved 05:00 UTC on 16 August 2026, filter purity 1.0
Most recent discoveries	7 August 2026 (Serengeti Estates), 2 August 2026 (DC Partner, Buzz Trading 104). All Krybit, all reported in W33
Feed tier	FREE v2, documented as delayed relative to PRO. Figures carry that caveat
Threat-level drivers	Three victim-confirmed breaches through suppliers; an exploited CVSS 10.0 flaw with public exploit code and 84 SA instances exposed; nine KEV items past their date

Group notes: no group claimed a South African victim this week. Twelve groups have been active against South Africa in the last 120 days: Black X, PrinzEugen, arcusmedia, cmdorganization, dragonforce, incransom, krybit, m3rx, payload, ransomhouse, stormous and thegentlemen.²² Krybit is the one to watch: three South African victims claimed between 2 and 7 August, after a single victim in the preceding four months, then a silent week. One quiet week does not establish the burst is over. The test set in W33 remains unanswerable, since what separates a deliberate African campaign from affiliate coincidence is temporal clustering of claims across countries and a week with no claims supplies no evidence either way. The wider point is that a quiet week changes the South African picture very little: the tally is cumulative and slow-moving, three of the four most recent listings are unconfirmed, and this week's harm arrived entirely outside the leak-site channel. An organisation watching only leak sites would have recorded a week with nothing in it.

7. OSINT EXPOSURE & ATTACK SURFACE

All figures here are VERIFIED South African exposure counts retrieved at 05:00 UTC on 16 August 2026.⁷ They count instances of a product reachable from the internet, identifiable by fingerprint, and already indexed by Shodan. That last condition matters: Shodan scans on its own cycle and does not see everything, so each figure is a floor rather than a census, and the true exposed population is larger by an unknown margin. They are exposure counts: the vulnerability filter is unavailable on this plan, and no figure should be read as "N South African systems vulnerable to CVE-X". Results that failed fingerprint corroboration are held back, and organisation-level facets are never published, because naming a South African company as running an exposed appliance in a document distributed without restriction is targeting information.

7.1 Metabase: 84 Instances Exposed in South Africa

The panel gained a Metabase query this week, promoted automatically from the KEV addition of CVE-2026-72898 and confirmed against the product facet before use.⁷ A country-scoped product match returns 84 South African instances with the facet resolving entirely to the Metabase label, so the fingerprint is unambiguous. The port distribution is informative: 37 on 443, 25 on 3000, 11 on 80, and a tail on 30001 and 444.⁷ Port 3000 is the application default, and its presence on the public internet in that quantity indicates instances stood up directly rather than behind a managed reverse proxy, which is the

pattern most likely to leave the vulnerable endpoint reachable and least likely to have an ingress log to check it against. The count includes instances on fixed builds and instances below 1.58 which were never affected, and excludes Metabase Cloud tenants, whom the vendor patched.

7.2 The Standing Exposure Panel

Fortinet FortiGate	2,493. Facet resolves across model variants; free-text 'fortigate' independently returns 1,779
Exposed RDP (port 3389)	7,778 services, of which 7,209 carry the Remote Desktop Protocol label
Exposed port 445	4,481 services on that port. Only 154 carry a Samba label, so read these as services on port 445 rather than as identified SMB servers
Microsoft SharePoint on-prem	498, http.component match. Free-text returns 2 and is wrong: component index and banner text are different indexes
Apache Tomcat	836. CVE-2026-34486 is reachable via the Tribes clustering receiver on TCP 4000 rather than the web port, so read this as an exposure count
Cisco ASA WebVPN	357, corroborated by product facets and by 322 sitting on port 443
SonicWall, all products	2,593, summing five product strings because Shodan rejects an OR of product filters. Cannot be narrowed to the SMA 1000 line
Metabase	84, new to the panel this week, derived from CVE-2026-72898
Others tracked	Citrix Netscaler 99, WordPress 351 (a floor), IBM Langflow 42

Two entries are withheld and the reason matters. The Arista VeloCloud query returned zero by product match and zero by free text, and is held at PROVISIONAL rather than published. Zero is the result a wrong fingerprint produces, and an earlier edition nearly published a near-absence as intelligence on exactly that basis, before the correct SharePoint component query returned 316 against a free-text result of 2. A genuine near-absence of on-premises VeloCloud Orchestrator here is plausible and will not be asserted until a second method agrees. Separately, no South African figure is published for this week's Cisco ASA and FTD KEV entry: the catalogue product string has no corresponding Shodan label and three fingerprinting approaches returned nothing, so it is held for manual fingerprinting.⁷ The 357 ASA WebVPN figure above is a different, independently corroborated query and does not stand in for it.

7. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 16 August 2026. <https://www.shodan.io/>

8. REGULATORY & POLICY

8.1 Section 22 in Practice: Three Notifications, One Silent Regulator

Three South African organisations exercised POPIA section 22 in three different ways within six days. LEGO Certified Stores South Africa issued a written notice to data subjects citing section 22(1)(b) by name, describing the compromise, the likely consequences, the measures taken and a named Information Officer

as the point of contact, which is a good working model of what the section asks for.¹ Euphoria Telecom reported to the Information Regulator and notified customers, and said so on the record.⁹ Toyota South Africa Motors notified affected customers and stated that relevant authorities and regulators were engaged.⁸

Section 22 requires notification both to the Regulator and to affected data subjects, and only Euphoria stated plainly that it had done the first; no inference is drawn from the LEGO notice's silence, and Toyota's wording, that authorities and regulators were engaged, is not the same statement. The Regulator's own publication record is measurable and is measured here. Its media statements index carries a 2026 section holding eleven entries, the most recent being the enforcement notices issued on 2 June 2026 for contraventions of POPIA and PAIA by public and private bodies.²⁶ That is seventy-six days before this report, ten weeks and six days, which the KPI table rounds to eleven. The Regulator therefore does publish, and does enforce: the June statement is an enforcement action, not an announcement. What it has not published is anything about the breaches confirmed in the past fortnight, in a week when one South African organisation stated it had notified the Regulator and a second said regulators were engaged.

8.2 Who to Call: South African Incident Response Contacts

This report has repeatedly told readers to notify the Information Regulator without telling them who to call for incident response. The Regulator is a compliance destination rather than a responder. The six teams below are registered with FIRST and are the constituency-appropriate first technical contacts.²⁷ Identify which covers you before you need it; the worst time to look up a telephone number is during an encryption event.

Cybersecurity Hub (CSHUB-CSIRT)	National CSIRT. Constituency: government, private and public sectors. https://www.cybersecurityhub.gov.za/
ECS-CSIRT, State Security Agency	Electronic Communications Security CSIRT. Constituency: government and military. http://www.ssa.gov.za/csirt.aspx
SA NREN CSIRT	Constituency: research and education. https://csirt.sanren.ac.za/
UCT CSIRT	University of Cape Town. Constituency: research and education. https://csirt.uct.ac.za/
SBG CSIRT	Standard Bank Group. Constituency: internal to the group
Vodacom Group Cyber Intelligence Centre	Constituency: ISP customer base. https://www.vodacom.co.za

8.3 The Supplier Question POPIA Already Answers

Every South African incident confirmed this week involved an operator or a platform, and POPIA is clearer on this than most organisations behave as though it is. Section 21 requires a responsible party to have a written contract with an operator obliging it to establish and maintain the security measures required by section 19, and the responsible party remains accountable for the processing. The practical gap is not the law: most operator agreements express notification as "without undue delay" and say nothing about the operator's own suppliers. In the LEGO chain the defect sat in a tool the operator used internally, a layer a

standard operator agreement typically does not reach at all. The single question worth asking this week is whether your operator agreements impose a notification deadline in hours and whether they extend to incidents at the operator's own suppliers.

26. Information Regulator (South Africa), Media Statements index, retrieved 16 August 2026.
<https://inforegulator.org.za/media-statements/>

27. ransomware.live, South African CSIRT directory, endpoint /csirt/ZA, 6 teams, sourced from FIRST, retrieved 16 August 2026.
<https://www.ransomware.live/>

9. WEEKLY THREAT HUNT & IOCs

Seven missions. Three P1 cover the actively exploited software behind this week's South African harm and the estate-management software still under hands-on intrusion; two P2 cover the remaining KEV additions and the SMS platform abuse pattern; two P3 cover the consumer fraud following the week's credential and contact-data exposures. Indicators come from vendor advisories and named responder reporting; the per-group indicator feed returned data only for groups with no South African activity this week. Where a mission has no atomic indicators it says so rather than inventing any. A machine-readable export of 46 sourced indicators accompanies this report as iocs_w34.csv; TH-03 and TH-07 contribute none, having no atomic indicator to export.

TH-2026-W34-01: Metabase CVE-2026-72898 Exploitation and Admin Takeover	P1 CRITICAL: CVSS 10.0; zero-day; public PoC from 10 Aug; SA victim confirmed
Hypothesis: An unauthenticated attacker has injected SQL through the password reset endpoint of a self-hosted Metabase instance, obtained administrator access, and stolen the stored credentials for every connected database. The instance need not be internet facing; it needs only to be reachable from wherever the attacker is. MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1552.001 (Credentials In Files), T1078 (Valid Accounts), T1213 (Data from Information Repositories), T1041 (Exfiltration Over C2 Channel). IOCs: The vendor's compromise signature is a sequence rather than a single string: POST /api/session/reset_password returning HTTP 400, followed by GET /api/user/current returning HTTP 200. Exploit bodies carry an undocumented user-id key beside the expected token and password keys, with a nested raw key containing SQL, for example {"token":"x","password":"y","user-id":{"raw":"..."} }. Version is readable unauthenticated at GET /api/session/properties. Affected builds are 1.58 and above, below the fixed releases. Data Sources: Metabase application logs, reverse proxy and ingress logs, WAF request bodies, application database audit logs, outbound netflow, and authentication logs on connected databases. Detection Guidance: Search ingress logs for the 400 then 200 sequence from one source address, and alert on any request to /api/session/reset_password whose body contains user-id. Upgrade or block the endpoint at the proxy on Monday 17 August. If the pattern is found, clear core_session to revoke sessions, audit API keys and administrator accounts, and rotate the credentials for every connected database. That last step is the one teams skip and the one that matters.	

TH-2026-W34-02: N-able N-central Post-Exploitation, Probable Storm-1175**P1 CRITICAL:** KEV due 6 and 7 Aug, LAPSED; hands-on intrusions inside this window

Hypothesis: An actor who gained administrative control of an N-central server before Hotfix 2 is still present. The vendor states the hotfix closes the entry path but does not evict an actor already inside, so patch status is not evidence of cleanliness and the hunt is for residual presence.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1136.002 (Create Account: Domain Account), T1098 (Account Manipulation), T1219 (Remote Access Software), T1003.001 (LSASS Memory), T1562.001 (Impair Defenses), T1199 (Trusted Relationship), T1486 (Data Encrypted for Impact).

IOCs: A newly created domain account named veeam, and password resets on existing domain administrator accounts. A registered service named Cloudflared, and a svchost.exe in a user's Documents directory; note that Sophos did not observe the svchost.exe artefact in the environment it examined and suggests it may be a renamed cloudflared.exe, so treat it as a pivot rather than proof. Nine addresses published by N-able, to which Sophos adds a tenth, 172.249.252.176: 173.249.252.200, 185.156.46.150, 23.234.94.43, 37.153.90.88, 37.19.210.32, 68.235.46.214, 68.235.46.235, 87.249.138.34, 92.118.112.181. Reported tooling: AnyDesk, SimpleHelp, TacticalRMM, Advanced IP Scanner, Mimikatz, and an EDR evasion utility used to disable Microsoft and Sophos protection. Microsoft attributes the activity to Storm-1175, deploying StormEncryptor.

Data Sources: N-central server logs, Windows Security Event Log on domain controllers for events 4720 and 4724, Windows Application Event Log on managed endpoints, EDR tamper alerts, perimeter netflow.

Detection Guidance: Enumerate every domain account created and every domain administrator password reset since 31 July, and treat an account named after a backup product as suspicious. Alert on agent stop or tamper events on servers. Apply Hotfix 2, build 2026.3.1.10, even where Hotfix 1 was applied, and scope an investigation rather than closing on patch status where the hotfix was late. If you buy managed IT services, ask your provider whether they run N-central and when Hotfix 2 was applied.

TH-2026-W34-03: Business Intelligence Tools as Credential Concentrators**P1 CRITICAL:** architectural review; the SA harm this week came through this layer

Hypothesis: A reporting or business intelligence tool holds standing, long-lived credentials to production databases, is administered outside normal server hardening because an analytics or product team stood it up, and would give an attacker more data than any single application server. This is a review rather than a search for a known indicator, and it is P1 because it is the structural lesson of this week's confirmed breach.

MITRE ATT&CK: T1552.001 (Credentials In Files), T1213 (Data from Information Repositories), T1078 (Valid Accounts), T1530 (Data from Cloud Storage). Initial access varies by product, and is T1190 where the tool is internet facing.

IOCs: No atomic indicators; this mission produces an inventory. Collect every BI, reporting, dashboarding and data-warehouse client in the estate, self-hosted or SaaS; the database account each authenticates with; that account's privilege level; whether the credential has ever been rotated; and whether the tool is reachable from the internet.

Data Sources: Asset inventory, cloud service enumeration, database user and grant tables, external reachability scans, expense records for analytics SaaS subscriptions.

Detection Guidance: Query the grant tables on every production database and list the accounts used by reporting tools. The common finding is a read-everything account with no row-level restriction and a password set at installation. Reduce those grants, set a rotation schedule, and put the tool behind external authentication. Expense records find the analytics SaaS nobody told security about. The board-facing output is one list: which tools read customer data, who operates them, and when credentials changed.

TH-2026-W34-04: The Two KEV Additions With No Published Indicators**P2 HIGH: CVE-2026-20349 (OVERDUE +3) and CVE-2026-68820; behavioural hunting only**

Hypothesis: Two of this week's three KEV additions have no published exploit indicators, addresses or samples, so neither can be hunted by import. On Cisco ASA and FTD an unauthenticated remote attacker forces a reload and denies remote access to everyone terminating on the appliance. On Windows an attacker who already has low-privilege execution uses a use-after-free in the Ancillary Function Driver for WinSock to reach SYSTEM, the step that turns any of the footholds elsewhere in this edition into a domain problem.

MITRE ATT&CK: T1499 (Endpoint Denial of Service) and T1190 (Exploit Public-Facing Application) for the Cisco flaw; T1068 (Exploitation for Privilege Escalation) and T1055 (Process Injection) for the Windows flaw.

IOCs: None published for either CVE, and none are invented here. Cisco observables: unexplained reloads, crash dumps referencing memory inspection, and reloads with no preceding administrative session. Windows observables: a process reaching SYSTEM integrity without an expected parent, and afd.sys interactions from unusual user-mode processes. The 357 Cisco ASA WebVPN portals exposed in South Africa are an exposure count for the family rather than a count of vulnerable appliances, and no South African figure exists for the catalogue product string itself, which has no Shodan fingerprint.

Data Sources: ASA and FTD syslog and crashinfo, SNMP availability monitoring, VPN session logs; EDR process and token telemetry, Windows Security Event ID 4688 with parent process recorded, Sysmon events 1 and 10.

Detection Guidance: Correlate every unplanned reload in the past fortnight against administrative session logs; a reload with no preceding authenticated session is what to escalate, and it looks like a hardware fault in a monitoring dashboard. Where a remote-access outage would be material, confirm a secondary path exists that does not terminate on the same appliance, since the practical mitigation for a denial of service against one concentrator is a second way in. For the Windows flaw, apply the August updates before 25 August and hunt token elevation whose parent is a browser, Office application, script host or anything under a user profile. The vector is local, so exposure counts are irrelevant and the population at risk is every Windows host; prioritise internet-facing servers, VDI and jump hosts, and the workstations of users with administrative rights elsewhere.

TH-2026-W34-05: Bulk SMS Platform Account Abuse**P2 HIGH: confirmed SA incident; fraudulent messages from a legitimate sender identity**

Hypothesis: An attacker with access to an organisation's bulk SMS platform account sends fraudulent messages from the organisation's own registered sender identity. Recipients apply every check they have been taught and all of them pass, because the message genuinely came from the right sender. The security team usually has no telemetry here, because the platform is contracted and operated by marketing.

MITRE ATT&CK: T1586.002 (Compromise Accounts, applied to messaging platform accounts), T1078 (Valid Accounts), T1656 (Impersonation), T1598 (Phishing for Information).

IOCs: No indicators are published for the Toyota South Africa incident and the provider has not been named, so there is nothing atomic to import. Gather from your own provider: send volumes by campaign and hour, sender identities used, API key and login history with source addresses, and any campaign created outside the approval workflow. In the confirmed case the lure was a purported gambling promotion.

Data Sources: Bulk SMS provider portal and API audit logs, marketing automation logs, customer complaint and call-centre records, brand monitoring.

Detection Guidance: Obtain read access to your SMS provider's audit log this week; for most security teams that is the entire finding, because they do not have it. Alert on volume outside business hours, on any new sender identity, and on API key use from an unfamiliar address. Enforce multi-factor authentication on platform accounts, rotate API keys like production secrets, and establish who in marketing can lock a compromised account at 02:00, because locking the account was the containment step in the confirmed case.

TH-2026-W34-06: SIP Credential Abuse and International Toll Fraud

P3 MEDIUM: confirmed SA telephony incident; loss is realised in hours

Hypothesis: Compromised SIP or extension credentials are used to place high volumes of calls to premium-rate international destinations, overnight or across a weekend, with the charge landing on the account holder. Unlike a data breach the loss is immediate and financial, and the first indication is usually the bill.

MITRE ATT&CK: T1078 (Valid Accounts), T1496 (Resource Hijacking), T1657 (Financial Theft).

IOCs: None published for the Euphoria Telecom incident, and the company describes the credential exposure as a risk rather than a confirmed loss, so nothing is imported as fact. The detectable pattern is generic and reliable: call detail records showing a sharp rise in international destinations outside business hours, repeated short-duration calls to the same high-cost country codes, and one extension registering from more than one source address or geography.

Data Sources: PBX and SIP trunk call detail records, SBC registration logs, provider billing alerts, firewall logs for SIP signalling on UDP and TCP 5060 and 5061.

Detection Guidance: Set a hard cap on international dialling per extension and alert on any hour exceeding it, the control that turns a six-figure loss into a four-figure one, and alert on one extension registering from two geographies within a short interval. Rotate SIP credentials on suspicion rather than after confirmation, since rotation is cheap and delay accrues hourly.

TH-2026-W34-07: Brand-Impersonation Phishing on Leaked Contact Data

P3 MEDIUM: predicted by the victim's own notice; SA retail and automotive data exposed

Hypothesis: Email addresses and mobile numbers taken from a named South African retail or automotive brand are used to run impersonation campaigns against those customers. The attacker knows the recipient is a genuine customer of a specific brand, which removes the largest source of friction in mass phishing.

MITRE ATT&CK: T1566.001 and T1566.002 (Spearphishing), T1656 (Impersonation), T1583.001 (Acquire Infrastructure: Domains).

IOCs: No campaign indicators have yet been observed using this dataset, and none are invented here. Monitorable artefacts: newly registered domains combining the brand name with terms such as loyalty, rewards, points, service or booking; certificate transparency entries for the same; and inbound mail displaying the brand name without passing DMARC alignment.

Data Sources: Certificate transparency logs, newly registered domain feeds, DMARC aggregate reports, secure email gateway telemetry, customer complaint channels.

Detection Guidance: Move DMARC to a reject policy for the affected brands, since that is the only control that stops exact-domain spoofing rather than merely reporting it, and monitor certificate transparency for brand-adjacent registrations weekly. Where customer contact data has been exposed, publish a single verification channel and tell customers to use it, which is what the LEGO Certified Stores notice does. Advice to spot a badly written message should be retired; it no longer describes what customers receive.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. Patch self-hosted Metabase on Monday 17 August, then run the compromise check. Upgrade to 63.5, 62.9, 61.11, 60.17, 59.21 or 58.24, or block `/api/session/reset_password` at the proxy until you can. Then search ingress and application logs for a POST to that endpoint returning 400 followed by a GET to `/api/user/current` returning 200. If the sequence is present, clear `core_session` to revoke sessions, audit API keys and administrator accounts, and rotate the credentials for every connected database. Public exploit code has been available since 10 August.

2. Inventory every tool in the estate that holds standing database credentials. Query the grant tables on your production databases and list the accounts used by reporting, dashboarding and integration tools, then check privilege level and last rotation date. The recurring finding is a read-everything account created at installation and never changed. This is TH-2026-W34-03, and it is the mission most likely to find something in an estate with no Metabase at all.

3. Treat N-central patch status as insufficient evidence, and apply the Cisco ASA and FTD fix. The vendor states Hotfix 2 closes the entry path but does not remove an actor already inside. Enumerate domain accounts created and domain administrator passwords reset since 31 July, look for an account named veeam, a service named Cloudflared and a svchost.exe under a user profile, and check the nine addresses published by N-able against perimeter logs, noting Sophos lists a tenth. On CVE-2026-20349, patch and review unplanned appliance reloads against administrative session logs; a reload with no preceding authenticated session is the only behavioural signal the flaw produces, and it looks like a hardware fault.

Management (CISO / Board)

1. Ask which suppliers hold your customer data and what they run it on, then put a notification deadline in hours into the contract. All three South African incidents confirmed this week reached the victim through a third party or landed on one, and in the most instructive case through a tool that third party used internally. POPIA section 21 already requires a written contract obliging an operator to maintain section 19 security measures, and the responsible party stays accountable regardless. What most agreements lack is a hard notification clock and any reach into the operator's own supply chain.

2. Stop treating patching speed as the headline metric. A one-day patch cycle did not prevent this week's loss, because the flaw was exploited before the vendor knew it existed. Patching speed is necessary and it is not enough on its own. The metrics that would have changed the outcome are about blast radius: how much data a single compromised tool can read, how many database credentials it holds, and how quickly they can be rotated.

3. Read the 92 per cent figure correctly, and identify your CSIRT. South Africa's share of African ransomware detections in INTERPOL's 2026 assessment is TrendAI telemetry for 2025 and measures where one vendor has sensors; leak-site counts put South Africa at roughly a fifth to a quarter of African listings, and neither is an incidence rate. Section 8.2 lists the six South African teams registered with

FIRST, since the Information Regulator is a compliance destination rather than a responder. And with two South African brands' customer contact details exposed this week, publish one verification channel and retire advice about spotting a badly written message.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 17th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a seventeenth consecutive week (9 August to 15 August 2026); the streak figure is corrected in this edition, see Correction 1 in Section 1. De-escalation to MEDIUM was considered on the strength of a week with no ransomware listing at all, and rejected: three organisations confirmed breaches, an actively exploited maximum-severity flaw has public exploit code and 84 exposed South African instances, and nine tracked KEV items are past their remediation date. Escalation to CRITICAL was not close. No national-scale event occurred, no systemically important institution lost service, and the confirmed harm was contact data rather than payment data, credentials or operational disruption.

Rationale

- **Three confirmed breaches, all on the supply chain.** LEGO Certified Stores South Africa notified data subjects under section 22 after contact details were taken through its marketing operator's internal reporting tool; Toyota South Africa Motors confirmed possible exposure through a bulk SMS provider whose account sent fraudulent messages from a legitimate sender identity; and Euphoria Telecom, a supplier of cloud telephony to South African businesses, confirmed unauthorised access to its own environment and notified the Information Regulator.
- **A maximum-severity flaw with a South African victim, public exploit code and local exposure.** CVE-2026-72898 scores 10.0, was exploited as a zero-day before disclosure, entered KEV on 11 August with a 14 August due date now three days past, has public proof-of-concept code from 10 August, and has 84 instances exposed in South Africa.
- **Hands-on intrusion continuing in managed service provider software.** Two independent responders reported N-central intrusions during this window, including domain administrator password resets, a domain account named after a backup product, and disabling of endpoint protection. Microsoft assesses the actor is Storm-1175, deploying a new encryptor called StormEncryptor.
- **An overdue backlog that keeps deepening, and no regulatory signal against a rising notification load.** Nine tracked KEV items sit past their remediation date, the deepest at thirty-one days, and two of this week's three additions expired before publication. One South African organisation said this week that it had notified the Information Regulator, a second said regulators were engaged, one issued a model section 22 notice, and the Regulator has published nothing about any confirmed breach of the past fortnight, subject to the caveat in Section 8.1.
- **Against escalation: a genuinely quiet ransomware week.** No South African victim was listed between 9 and 15 August, the tally is unchanged at 119, and Krybit's three-victim burst did not continue. That

argues for a lower level, and it is outweighed by three confirmed breaches arriving through a channel the leak-site tally does not observe.

Next-Week Watch (W35)

- **Marsello and the rest of its South African customer base.** Whether Marsello publishes a statement, and whether another South African brand notifies over the same incident. What separates a single-brand event from a multi-brand one is a second section 22 notice naming Marsello.
- **The aggregator map discrepancy.** The public map page showed 105 records against 119 from the API on 16 August. A record-level comparison separates the two explanations: if the fourteen missing entries are the most recent it is a cache, if scattered the two views apply different rules.
- **The Information Regulator on this fortnight's breaches.** The Regulator last published on 2 June 2026, and that was an enforcement action rather than an announcement, so silence here is not inactivity. The observation to watch for is any statement, assessment or enforcement notice naming LEGO Certified Stores, Toyota South Africa Motors, Euphoria Telecom, DC Partner or Fidelity Services Group, all of which either notified it or said regulators were engaged.
- **Metabase exploitation reaching South African victims directly.** The harm so far arrived through a foreign operator. With 84 exposed local instances and public exploit code, watch for a South African organisation disclosing a compromise of its own instance, which would move this from a supply-chain story to a domestic exploitation one.
- **Whether N-able distinguishes a bypass from a second path.** The vendor's phrase, "a related attack path", is compatible with both. The observation that settles it remains a victim compromised while running build 2026.3.1.7, and this is the second week the test has gone unanswered.
- **Krybit after a silent week, and the open South African listings.** Whether claims resume and whether new African victims cluster in time; the temporal-clustering test set in W33 stays unanswerable until there are further claims. In the same line: whether any DC Partner dataset surfaces, whether the National Credit Regulator responds to a confirmed breach at an entity it accredits, and whether Serengeti Estates or Buzz Trading 104 moves off CLAIMED.
- **Toyota's SMS provider.** Whether the provider is named, by the company once the investigation closes or by another affected brand. Until it is, no other South African organisation can tell whether it shares that supplier.

12. OSINT SOURCES CONSULTED

All sources are TLP:WHITE and publicly accessible except entry 1, numbered in order of first citation. Every cited URL was retrieved and confirmed to contain the claim attributed to it, on 16 August 2026. **Collection notes.** The feed run completed at 05:03 UTC on 16 August 2026 and passed its integrity check with a clean exit; ransomware.live returned 119 records of which 119 were South African, a filter purity of 1.0. The press, YARA, ransom note and negotiation endpoints returned nothing. Two Shodan queries were held back: Arista VeloCloud, an unproven fingerprint rather than an absence, and the Cisco ASA and FTD product string, which has no Shodan label. Entry 1 is a primary document received by the compiler as an affected customer, with the Information Officer's contact details not reproduced. Entry 26 is the Regulator's media

statements index, read for the 2026 section; see Section 8.1. **Attribution policy.** Where a story was broken by a publication, this report names who broke it, links to them, and summarises only what the intelligence judgement requires rather than reproducing the account. Readers who want the full story should follow the credit link and read it at the source. This applies to every publication cited here, South African and international alike. **Single-source disclosure.** Alternative sources were sought for every South African claim in this edition, and primary or independent reporting is used wherever it exists. Four sets of facts remain sourced to one South African publication because no other account of them could be found: the Toyota South Africa Motors incident in full; the Euphoria Telecom incident in full; DC Partner's 7 August confirmation and the FNB response; and the Fidelity Services Group chief executive's quoted statements. The LEGO Certified Stores facts rest on the received section 22 notice, with that reporting as corroboration rather than as the source. Readers should weight the four single-sourced items accordingly.

1. LEGO Certified Stores South Africa, section 22 POPIA data breach notification to affected customers (14 August 2026). Received primary document, not published online.
2. MyBroadband, Lego Certified Stores South Africa hit by zero-day hack of third-party database provider (14 August 2026). <https://mybroadband.co.za/news/security/662655-lego-certified-stores-south-africa-hit-by-zero-day-hack-of-third-party-database-provider.html>
3. SecurityWeek, Metabase Patches Vulnerability Exploited as Zero-Day (10 August 2026), quoting the vendor advisory GHSA-vwrf4-m7j8-wcjf. <https://www.securityweek.com/metabase-patches-vulnerability-exploited-as-zero-day/>
4. The Hacker News, Metabase Zero-Day Exploited in Wild Allows Admin Access Without Authentication (8 August 2026, updated 11 August). <https://thehackernews.com/2026/08/metabase-zero-day-exploited-in-wild.html>
5. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.14, released 14 August 2026, retrieved 16 August 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
6. NVD CVSS base scores with scoring source, retrieved 16 August 2026. <https://nvd.nist.gov/>
7. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 16 August 2026. <https://www.shodan.io/>
8. MyBroadband, South African Toyota customers' personal info possibly leaked after SMS provider breach (14 August 2026). <https://mybroadband.co.za/news/security/662372-south-african-toyota-customers-personal-info-possibly-leaked-after-sms-provider-breach.html>
9. MyBroadband, Euphoria Telecom contains breach after it suffers cyberattack (13 August 2026). <https://mybroadband.co.za/news/security/662245-euphoria-telecom-contains-breach-after-it-suffers-cyberattack.html>
10. INTERPOL, African Cyberthreat Assessment Report 2026, released 3 August 2026, PDF cover dated June 2026. Figure 4, Ransomware detections by country in 2025, Source: TrendAI. <https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026>
11. IOL, South Africa named Africa's cybercrime hotspot (4 August 2026). <https://iol.co.za/news/crime-and-courts/2026-08-04-south-africa-named-africas-cybercrime-hotspot/>
12. eNCA, SA 'overwhelmingly' targeted by cybercriminals says Interpol (5 August 2026). <https://www.enca.com/news-top-stories/sa-overwhelmingly-targeted-cybercriminals-says-interpol>
13. 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>
14. Alibaba, fastjson release 1.2.84 (29 July 2026). Repository archived the same day. <https://github.com/alibaba/fastjson/releases/tag/1.2.84>
15. Alibaba, Security Advisory: Remote Code Execution in fastjson 1.2.68 to 1.2.83, last edited 21 July 2026. <https://github.com/alibaba/fastjson2/wiki/Security-Advisory:-Remote-Code-Execution-in-fastjson-1.2.68%E2%80%931.2.83>
16. Wiz Research, Inside the Metabase SQLi: Exploited in the Wild (10 August 2026). <https://www.wiz.io/blog/inside-the-metabase-sqli-exploited-in-the-wild>
17. N-able, N-central Security Update, August 10 2026 (published 9 August 2026). <https://www.n-able.com/blog/n-central-security-update-august-10-2026>
18. Help Net Security, CVE-2026-18577: N-central Hotfix 2 and what MSPs must do now (10 August 2026). <https://www.helpnetsecurity.com/2026/08/10/cve-2026-18577-n-central-hotfix-2-msps/>
19. MyBroadband, One of four payment agents accredited by the National Credit Regulator suffers 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>
20. DC Partner (Pty) Ltd corporate website, NCR registration and company details, retrieved 16 August 2026. <https://www.dcpartner.co.za/>
21. MyBroadband, South Africa'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>
22. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 119 records at filter purity 1.0, retrieved 05:00 UTC on 16 August 2026. <https://www.ransomware.live/>
23. JetBrains, CVE-2026-63077 update (7 August 2026). <https://blog.jetbrains.com/teamcity/2026/08/cve-2026-63077-update/>
24. The Hacker News, Progress Kemp LoadMaster flaw hits CISA KEV catalogue (8 August 2026). <https://thehackernews.com/2026/08/progress-kemp-loadmaster-flaw-hits-cisa.html>
25. FIRST, Exploit Prediction Scoring System scores, retrieved 16 August 2026. <https://www.first.org/epss/>
26. Information Regulator (South Africa), Media Statements index, retrieved 16 August 2026. <https://info regulator.org.za/media-statements/>
27. ransomware.live, South African CSIRT directory, endpoint /csirt/ZA, 6 teams, sourced from FIRST, retrieved 16 August 2026. <https://www.ransomware.live/>

TLP:WHITE. Distributable without restriction. Compiled from open sources and from feeds retrieved under the compiler's own credentials, and identifies no South African organisation as running a specific exposed system.