



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 37 | 30 August – 5 September 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W37 | Classification: TLP: CLEAR

Published Monday 7 September 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 (W37)
- 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, 20th consecutive week (30 August - 5 September 2026)

Story 1. Rand Water, the bulk water utility that supplies more than 16 million people across Gauteng and parts of the Free State, North West and Mpumalanga, confirmed that its network was breached and that servers were damaged. The utility disclosed the incident on 3 September in a statement to holders of its listed debt on the JSE, saying it was responding to a cyber security incident affecting certain information technology systems while water treatment, water quality control and bulk supply remained fully operational.^{1,2} Its debt officer, Lucky Ncobela, told ITWeb that the intrusion was detected at night, that attempts to block it came too late, and that the utility is now running from its disaster recovery site in Centurion while equipment at its main site is sanitised and replaced.¹ No actor has been named and no ransomware family has been attributed. This is the first confirmed compromise of South African bulk water infrastructure this series has carried. First reported by [MyBroadband](#) on 2 September 2026.

Story 2. The Information Regulator held the media briefing this report flagged as a watch item and put a number on South African breach volume for the first time in this series: more than 8,000 security compromise notifications received to date, of which 1,220 arrived since the start of the 2026/27 financial year in April, on a trajectory the chairperson expects to exceed 3,000 for the year.³ Advocate Pansy Tlakula called the position very alarming and said the Regulator is not sure that public and private bodies are as alarmed as it is. An enforcement notice was issued against the South African Bureau of Standards after its 2024 ransomware attack, giving it 90 days from receipt to revise policies, run personal information impact assessments and implement security measures.^{3,4} The watch item resolves in a specific way that matters to the KPI: the Regulator announced a great deal and published nothing. The count runs from the Gauteng Department of Health enforcement notice of 8 June 2026, the last substantive instrument it published, and thirteen weeks separate that from this publication date; the enforcement-notices register itself carries nothing later than 16 April 2025.^{5,6}

Story 3. Ten vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 31 August and 4 September, and five were past their remediation date on the day this report was published.⁷ The heaviest pair is SonicWall SMA 1000: CVE-2026-83548, a pre-authentication server-side request forgery scored 10.0, and CVE-2026-83549, a post-authentication command injection, which Rapid7 states can be chained so that the command injection is reachable without credentials.^{8,9} SonicWall's own notice says the vulnerabilities have been confirmed as actively exploited in the wild and tells customers who find indicators to re-image the appliance rather than patch it.⁸ That is the third exploited SMA 1000 chain this report has tracked, and the July pair remains overdue by fifty-two days.

Also this week. DireWolf listed Cartrack Holdings on 2 September, claiming 100 GB, the only new South African leak-site entry in the window and the group's first South African victim.¹⁰ Neither Cartrack nor its parent Karoo000 has made any public statement, so the item is rated CLAIMED.¹¹ There is no correction owed to a prior edition this week.

KPI Dashboard

Metric	Current (W37)	Prior (W36)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (20th week)	FLAT
ransomware.live SA cumulative	125	124	+1	UP
SA claims dated inside the window	1	2	-1	DOWN
Window claims surviving the nationality check	1 of 1	2 of 2	n/a	n/a
SA breaches confirmed by the victim	2	1	+1	UP
New CISA KEV additions	10	11	-1	DOWN
KEV adds already overdue at publication	5	6	-1	DOWN
KEV adds with a published VERIFIED SA exposure figure	1 of 10	3 of 11	-2	DOWN
Corrections issued to prior editions	0	0	0	FLAT
Weeks since last IR substantive publication	13	12	+1	UP

Two notes on the table. The exposure row is renamed because it now counts figures actually published: the collection returned 4,041 internet-facing LiteLLM instances in South Africa and that figure is withheld, for the reasons in Section 7.2. The victim-confirmed row counts Rand Water and Implats, the second surfacing in audited financial statements rather than in a breach notice.

W37 KEY FRAMING: the week's question for a board is not which software you run, which was last week's question, but who is obliged to tell you when something breaks. Rand Water disclosed a confirmed intrusion at Africa's largest bulk water utility, and it did so because it has listed debt on the JSE and therefore owes its bondholders a statement. A public body without listed instruments owes no equivalent disclosure, because South African law compels notification only where personal information is involved. In the same week the Information Regulator revealed that it holds over 8,000 breach notifications it does not publish, Implats acknowledged a breach in audited financial statements that ITWeb could not find on the Regulator's website, and the FSCA and Prudential Authority switched on a 24-hour material incident notification clock for financial institutions that applies over weekends. Three different disclosure regimes, one country, and only one of them produces anything a peer organisation can learn from. For a CISO the practical consequence is that the absence of reported incidents in your sector is not evidence of their absence, and your own assurance work cannot lean on it.

1. ITWeb, Hackers breach Rand Water's defences (4 September 2026). <https://www.itweb.co.za/article/hackers-breach-rand-waters-defences/Gb3BwMWaO4ov2k6V>

2. TechCentral, Cyberattack hits South Africa's biggest water utility (3 September 2026). <https://techcentral.co.za/rand-water-cyberattack/285746/>

3. ITWeb, InfoReg concerned by 'alarming' rate of data breaches (31 August 2026). <https://www.itweb.co.za/article/info-reg-concerned-by-alarming-rate-of-data-breaches/rxP3jqBE2ZLMA2ye>

4. Polity / Werksmans Attorneys, The regulator is watching: new enforcement signals for POPIA and PAIA compliance (1 September 2026). <https://www.polity.org.za/article/the-regulator-is-watching-new-enforcement-signals-for-popia-and-paia-compliance-2026-09-01>

5. Information Regulator of South Africa, Gauteng Department of Health enforcement notice, 8 June 2026, the anchor for the weeks-since-publication count.
<https://inforegulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>
6. Information Regulator of South Africa, enforcement notices register, nothing later than 16 April 2025, checked 6 September 2026.
<https://inforegulator.org.za/enforcement-notices/>
7. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.04, released 4 September 2026, retrieved 6 September 2026.
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
8. SonicWall, Product notice: SMA 1000 series affected by multiple vulnerabilities, SNWLID-2026-0016 (1 September 2026). <https://www.sonicwall.com/support/notices/product-notice-sma-1000-series-affected-by-multiple-vulnerabilities-snwlid-2026-0016/kA1VN000002AXmQOAW>
9. Rapid7, Critical SonicWall SMA1000 vulnerabilities CVE-2026-83548 and CVE-2026-83549 exploited in the wild (2 September 2026). <https://www.rapid7.com/blog/post/etr-critical-sonicwall-sma1000-vulnerabilities-cve-2026-83548-cve-2026-83549-exploited-in-the-wild/>
10. ransomware.live, victim record: Cartrack Holdings, DireWolf, discovered 2 September 2026.
<https://www.ransomware.live/id/Q2FydHJhY2sgSG9sZGluZ3NAZGlYXxdvbGY=>
11. Karooooo Limited, JSE SENS announcements index, most recent entry 28 July 2026, checked 6 September 2026.
<https://karooooo.com/jse-sens-announcements/>

TOP 3 ACTIONS THIS WEEK

1. Deal with SonicWall SMA 1000 on Monday 7 September, and treat patching as insufficient.

CVE-2026-83548 and CVE-2026-83549 were both due on 5 September, so they are already two days overdue. The fixed builds are 12.4.3-03526 and 12.5.0-02952. SonicWall's remediation goes beyond the patch: contact SonicWall Support for an indicator review, and where indicators are found, re-image or re-deploy the appliance, change every user and administrator password and reset TOTP tokens. If your organisation still has CVE-2026-15409 or CVE-2026-15410 outstanding from July, that appliance has been reachable and exploitable for fifty-two days and should be rebuilt regardless of what this week's patch does.

2. Check whether you run PaperCut, and check which emergency patch you are on.

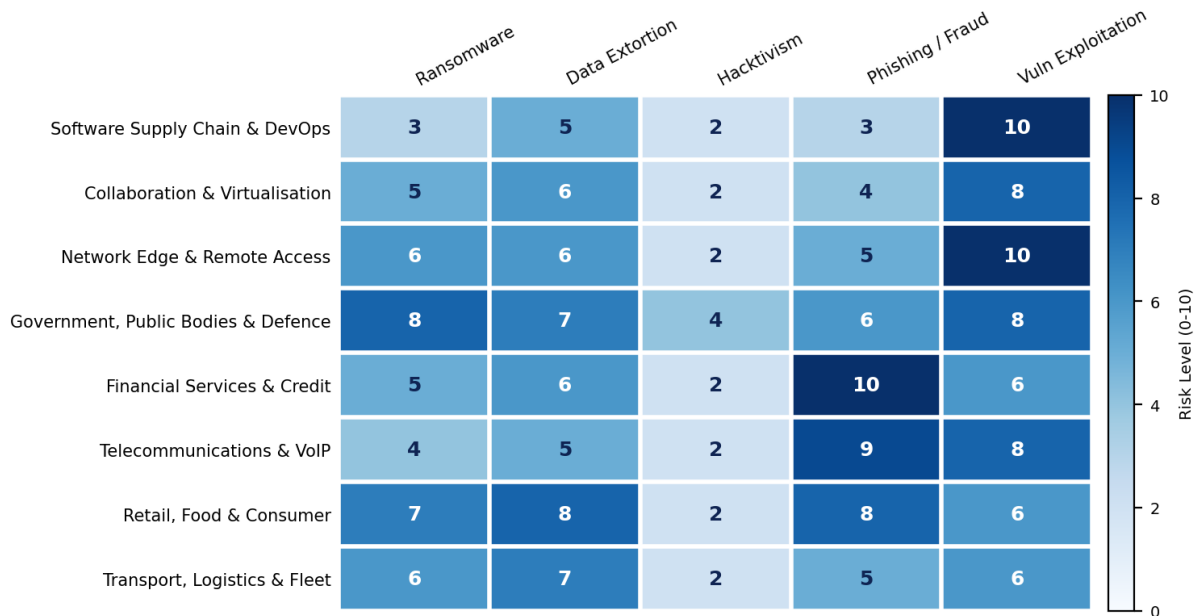
PaperCut NG and MF entered the catalogue on 31 August with a pre-authentication chain, and the vendor has now shipped three successive out-of-band releases because the first two were bypassed. Rapid7's guidance as at 1 September is explicit: an organisation running either the first or the second emergency patch is not fully protected and must apply the third. A Metasploit module for the chain is public, which moves this from targeted to commodity risk. Versions 23 and earlier have no patch and must be upgraded.

3. Ask your utilities, medical schemes and outsourced administrators what they would tell you.

Rand Water told the market because it has listed debt. Most of the third parties holding your data or running your processes have no equivalent trigger, and POPIA obliges notification only where personal information is compromised. Add a contractual notification clause with a stated hour count to the next three supplier renewals, and for regulated financial institutions align it with the FSCA and Prudential Authority 24-hour material incident template that took effect on 1 September 2026, since outsourcing the function does not outsource the obligation.

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 37 (30 August - 5 September 2026)



Methodology: each cell is an analyst score from 0 to 10 for the coming week, set from what this edition observed: leak-site listings with a South African tag that survives a nationality check, incidents confirmed by the organisation affected, catalogue additions affecting software the sector runs, VERIFIED South African exposure counts for that software, and reported fraud activity. It is a forward-looking prioritisation aid rather than a measurement, and a sector with no observation this week carries its prior score rather than dropping to zero.

One row retired, one row added. Research, Education and HPC is retired. Its score has been carried since the Lengau supercomputer matter, and the only item in this window touching that sector is a procurement story about the delayed replacement system, which is not a security observation.¹² Transport, Logistics and Fleet enters at 6 for ransomware, 7 for data extortion, 2 for hacktivism, 5 for phishing and fraud and 6 for vulnerability exploitation. It enters rather than rises: a Transport, Logistics and Courier row was carried in W35 at higher values and was retired in W36, so this is a re-entry at a lower score under a renamed label rather than a movement. The basis is that the window's only new South African leak-site listing is a transport-tagged one, Cartrack Holdings, and the sector now carries two open extortion claims in three weeks with The Courier Guy. The nationality check is applied to the sector tally as well as to the weekly count, which resolves a review note left open in W36: the aggregator holds three Transportation-tagged South African records for 2026, but one of them, Air Cote d'Ivoire, is Ivorian, so the true 2026 South African figure is two.¹³

Movements among the retained rows. Network Edge and Remote Access rises from 9 to 10 on vulnerability exploitation: two SonicWall SMA 1000 flaws entered the catalogue with the vendor itself confirming exploitation, on top of a July pair that has been overdue for fifty-two days.^{7,8} Government, Public Bodies and Defence rises from 7 to 8 on vulnerability exploitation, on the SABS enforcement notice arising from an earlier ransomware attack and on the public-sector security picture the Regulator

described at its briefing. No initial access vector has been published for the Rand Water intrusion, so that incident is not used to move this category.³ Hacktivism moves from 3 to 4 as a placeholder rather than a finding: the one motive assessment in the window reads the Rand Water intrusion as intended to bring systems down rather than to extort, that assessment is a third-party opinion and Section 3.1 says so, and with no actor named the category cannot be ruled out. It reverts if attribution arrives.¹⁴ Telecommunications and VoIP rises from 7 to 8 because Sangoma Switchvox, a small-business PBX platform, entered the catalogue with an unauthenticated SQL injection reaching remote code execution and a researcher honeypot recorded a genuine exploitation attempt on 30 August, the first day of this window.¹⁵ Retail, Food and Consumer rises from 7 to 8 on phishing and fraud after nine months of Hungry Lion customer credentials were found in stealer logs.¹⁶ Collaboration and Virtualisation falls from 9 to 8: nothing in that family entered the catalogue this week and the SharePoint chain is unchanged from last week's assessment. Software Supply Chain and DevOps holds at the maximum, with three of the ten additions landing on developer and AI infrastructure. Financial Services and Credit is unchanged, its phishing and fraud score already at the ceiling.

12. MyBroadband, R500-million replacement for South Africa's top supercomputer gathering dust (30 August 2026). <https://mybroadband.co.za/news/government/665077-r500-million-replacement-for-south-africas-top-supercomputer-gathering-dust.html>

13. ransomware.live, SA victim records, /v2/countryvictims/ZA, 125 records all tagged ZA, retrieved 05:00 UTC 6 September 2026. <https://www.ransomware.live/>

14. The Citizen, Forget poisoned water, a cyberattack's real threat to SA is empty reservoirs (4 September 2026). <https://www.citizen.co.za/news/forget-poisoned-water-a-cyberattacks-real-threat-to-gauteng-is-empty-reservoirs/>

15. Horizon3.ai, Off the hook: active exploitation of Sangoma Switchvox CVE-2026-9586 (1 September 2026). <https://horizon3.ai/attack-research/disclosures/cve-2026-9586-sangoma-switchvox-rce/>

16. ITWeb, Hungry Lion customer creds online for months (1 September 2026). <https://www.itweb.co.za/article/hungry-lion-customer-creds-online-for-months/6GxRKqYQEDZqb3Wj>

3. TOP SA INCIDENTS (W37)

Four incidents, and the evidence quality is better than the run of recent weeks. Two are confirmed by the organisation affected, one through a statement to bondholders and one through audited financial statements. One rests on technical analysis of credential data by a named vendor. Only one is an unsupported actor claim. They are set out strongest evidence first this week, because the confirmed utility compromise is the item a board needs to read.

3.1 INC-2026-W37-01: Rand Water, Network Intrusion and Server Damage [CONFIRMED]

Sector	Government, public bodies and defence; state-owned bulk water utility
Organisation	Rand Water, Africa's largest bulk water utility, supplying more than 16 million people across Gauteng and parts of the Free State, North West and Mpumalanga
Disclosure	Statement on the JSE Stock Exchange News Service, 3 September 2026, to holders of its listed debt securities
Confirmed	Network infiltrated, some servers reached and some damaged. Now operating from the disaster recovery site in Centurion while the main site is sanitised and equipment replaced

Not affected	Water treatment, quality control and bulk supply reported fully operational; treasury unaffected, having already been remote
Actor	None named, no ransomware family attributed. One external assessment reads the intrusion as intended to bring systems down rather than to extort
Confidence	CONFIRMED for the intrusion and server damage, on the SENS statement and the debt officer's account to ITWeb. The motive assessment is a third-party opinion, not a finding

Rand Water disclosed on 3 September 2026, in a statement to the JSE Stock Exchange News Service, that it was responding to a cyber security incident affecting certain information technology systems and that the matter was being investigated and managed with internal and external specialists. The same statement said critical operational activities, including water treatment processes, water quality control systems and bulk water supply operations, remain fully operational.¹ The first public account came a day earlier from MyBroadband, working from a tip-off, which reported that payment software and the geographic information system were affected, so vendors and contractors could not be paid and companies needing infrastructure build approvals could not be told where the pipes run.¹⁷ Rand Water's public response through Caxton's Parys Gazette on the same day emphasised that water quality and supply were unaffected and that its core delivery mandate continued uninterrupted.²

The operational detail came from the utility's debt officer, Lucky Ncobela, speaking to ITWeb: the intrusion was identified at night, staff tried to block it and were too late, and some servers were damaged. Rand Water is running its Centurion disaster recovery site as its main centre while it sanitises and replaces equipment at the primary site, and he noted plainly that without that site the utility would have been in serious trouble.¹ Alistair Pugin of @Celyntis, quoted in the same piece, assessed that the attack looked malicious in intent and aimed at bringing systems down rather than at ransomware, which is an outside reading of the utility's own description and is presented as such, not as attribution.

Two specialists quoted by The Citizen set out what a water-sector incident looks like when it goes further than this one did. Anna Collard of KnowBe4 notes that the risk is operators locked out of control systems while reservoirs draw down in hours rather than days, higher-lying areas losing pressure first and back-siphoning creating a contamination pathway; Bongani Majola of ScaryByte notes that write access to programmable logic controllers could in principle interfere with dosing or induce pressure surges.¹⁴ Neither is describing what happened here. Both read the reported facts, an IT compromise with operational technology untouched, as evidence that the segmentation between the two held, and Collard cautions against reading a national-importance target list into it: her assessment is that attackers pick off whoever left the door open. The sector context is real though. ITWeb notes the FBI warning of July 2026 that actors were targeting internet-facing programmable logic controllers in the water and wastewater sector and causing operational disruptions, alongside CISA's matching alert of 30 July 2026.^{1,18}

Detection relevance: no indicators have been published for this intrusion, so there is nothing actor-specific to hunt. TH-2026-W37-05 covers the generic case, being destructive intent and lateral movement towards an operational technology boundary.

3.2 INC-2026-W37-02: Implats, Cyber Breach Surfacing in Audited Financial Statements [CONFIRMED]

Sector	Manufacturing and mining
--------	--------------------------

Organisation	Impala Platinum Holdings, Implats
Disclosure	An audit and risk committee focus area for FY27 in the audited annual financial statements to June 2026, following a description in the 2025 ESG report as a limited impact breach to a managed operation's IT environment
Not stated	The affected operation, the date, the nature of the breach, whether data was compromised, any quantified impact. ITWeb reports it does not appear on the Information Regulator's website
Confidence	CONFIRMED that a breach occurred, on the company's own audited statements. Scope and timing are unstated and are not inferred here

Implats named a cyber breach as a focus area for its audit and risk committee in the audited annual financial statements to June 2026, having previously described it in its 2025 ESG report as a limited impact cyber security breach to a managed operation's IT environment; the audit and risk chair, Dawn Earp, refers to remediation of actions arising from the recent cyber incident.¹⁹ The company has not named the operation, given a date, described the mechanism, said whether personal information was involved or quantified the impact. It is carried here for one reason. In the same week that the Information Regulator said it holds more than 8,000 breach notifications and complained that responsible parties do not always report, a JSE-listed miner acknowledged a breach in audited statements that ITWeb could not find recorded with the Regulator. That is an observation about what is publicly visible rather than a finding that no notification was filed, because notifications reach the Regulator through an eServices portal it does not publish. The distinguishing observation would be a statement from Implats or from the Regulator, and neither exists. **Detection relevance:** none, for lack of technical detail; the item belongs to Sections 8 and 10, on disclosure practice.

3.3 INC-2026-W37-03: Hungry Lion, Nine Months of Exposed Customer Credentials [PROBABLE]

Sector	Retail, food and consumer; quick-service restaurant
Organisation	Hungry Lion, hungrylion.co.za
Technical finding	SOCRadar stealer-log analysis identified 23 records tied to hungrylion.co.za, 13 of them customer accounts, dated October 2025 to July 2026, all against consumer-facing self-service portals
Actor claim	A MedusaLocker leak-site listing, surfaced by GalaxyWarden, cites 111 locations across seven southern African countries and three point-of-sale systems
Dispute and response	KnowBe4 Africa, citing initial DarkNotify analysis, reads the same incident as point-of-sale records rather than customers' personal information. Hungry Lion was not available for comment
Confidence	PROBABLE for the credential exposure, on one credible source carrying named vendor analysis of actual stealer records. The leak-site listing and its scale claims remain CLAIMED, and the data class is contested

ITWeb reported on 1 September that SOCRadar's analysis of infostealer logs found 23 records associated with hungrylion.co.za, thirteen of them customer accounts, dated October 2025 to July 2026. That is

roughly nine months of continuous exposure, and the records point at consumer-facing self-service portals rather than corporate systems, which is why SOCRadar frames the risk as account takeover and says the exposure warrants an assessment of whether customers need to be notified under POPIA.¹⁶ The separate MedusaLocker listing carries much larger claims and those are the attacker's words. The disagreement in the same article is worth carrying rather than resolving: KnowBe4 Africa, working from initial DarkNotify analysis, reads the incident as point-of-sale records rather than customer personal information, while SOCRadar's finding concerns credentials in stealer logs, a different dataset reached a different way, so the two may be describing different halves. The observation that would settle it is a statement from Hungry Lion identifying which systems held the records the actor describes. **Detection relevance:** TH-2026-W37-06 covers credential-stuffing detection against consumer portals, which is the actionable half regardless of how the claim resolves.

3.4 INC-2026-W37-04: Cartrack Holdings, DireWolf Leak-Site Claim [CLAIMED]

Sector	Transport, logistics and fleet; vehicle telematics software
Named organisation	Cartrack Holdings, cartrack.co.za, wholly owned by Karooooo Limited (NASDAQ: KARO)
Actor and listing	DireWolf, a closed ransomware crew first observed in May 2025. Listed 2 September 2026 at 17:53 UTC, estimated attack date the same day
Actor claim	100 GB exfiltrated. A leak screenshot is present on the aggregator record; no sample dataset, file count or ransom figure is published
Corroboration	No media coverage located, no Karooooo press release and no JSE SENS announcement referencing a cyber incident, the most recent SENS entry being 28 July 2026
Confidence	CLAIMED. Threat-actor assertion only. No victim statement, no regulator filing, no independent confirmation

DireWolf listed Cartrack Holdings on 2 September 2026, claiming 100 GB of exfiltrated data and posting a leak screenshot.¹⁰ This is DireWolf's first South African victim in the aggregator's record and only its second African one, the other being a Tunisian freight company.¹³ It is also the only new South African listing indexed inside the window. There is one collection note worth stating: the country-scoped API record retrieved at 05:00 UTC on 6 September carried a null data size, while the site's own victim page for the same listing shows 100 GB. The figure quoted here is the one on the victim page, and it is the attacker's number either way.

Nothing corroborates the claim. No South African or international outlet has carried it, Karooooo's press-release index and its JSE SENS announcements index carry nothing about a cyber incident, and the most recent SENS entry is dated 28 July 2026.¹¹ The pattern is consistent with DireWolf's recent behaviour rather than distinctive to Cartrack: the group listed THQ Nordic on 30 August with a 335 GB claim and, as TechNadu noted, no encryption claim, no ransom figure and no sample data, screenshots or supporting files published alongside it.²⁰ A leak screenshot is present in the Cartrack case, which is more than that listing carried, and it is still the attacker's own artefact.

The tests are the ones the company can run against DireWolf's documented behaviour, set out in Section 4.1: the group is Windows-only, drops a ransom note named HowToRecoveryFiles.txt in every folder,

appends the .direwolf extension, clears Windows event logs in a loop and stages exfiltration through gofile.io.^{21,22} None of that requires waiting for the actor. **Detection relevance:** TH-2026-W37-01 carries the DireWolf hunt with sourced atomic indicators.

3.5 Also Observed, Not Attributed to an Attack

Cape Town's 10111 police emergency number went offline from the Maitland command centre and was reported on Wednesday 2 September. It is included here to be closed rather than left to inference: the chairperson of the Portfolio Committee on Police attributed the outage to broken equipment, outdated systems and staffing pressure, and no source has connected it to a cyber incident.²³ It belongs in this report only as availability context for public-sector technology in the same week as the Rand Water compromise, and it should not be counted as an incident.

3.6 Carryovers

- **Furniture Bargaining Council, Deadlock, W36.** No further update. The council's website still serves the preliminary notification of 24 August and circular 11-26 remains its latest, so the exfiltration claim stays CLAIMED and the encryption stays CONFIRMED. The circular makes no reference to POPIA section 22 or to the Information Regulator.²⁴
- **Rohloff Group, INC Ransomware, W36.** No development. The leak-site record still reads that full publication is coming, and no statement from the franchisee, KFC or Yum! Brands could be located. Stays CLAIMED.¹³
- **The Courier Guy, MedusaLocker, W35.** No development and no correction. The company's denial of 18 August stands unchallenged and unconfirmed. Stays CLAIMED.²⁵
- **Babcock Africa, The Gentlemen, W35.** No development. The company's update of 18 August remains the latest item on its news index. Stays CLAIMED.²⁶
- **Toyota South Africa Motors, W34.** The bulk SMS provider has still not been publicly named. Note a collection limit rather than a finding: the Toyota South Africa website is client-side rendered and could not be read here, so this is no publicly reported update rather than no update.²⁷
- **Lengau supercomputer, CHPC and CSIR, W36.** No follow-up on the cryptomining compromise. The only in-window item is a procurement story about the replacement system's components sitting in storage, which does not touch the compromise.¹²

17. MyBroadband, South Africa's largest bulk water utility allegedly crippled by cyberattack (2 September 2026).

<https://mybroadband.co.za/news/security/665683-south-africas-largest-bulk-water-utility-crippled-by-cyberattack.html>

18. CISA, Water and wastewater systems sector urged to protect OT against activity targeting PLCs (30 July 2026). <https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs>

19. ITWeb, Implats pushes AI as it addresses cyber breach (3 September 2026).

<https://www.itweb.co.za/article/implats-pushes-ai-as-it-addresses-cyber-breach/Gb3BwMWaOwpv2k6V>

20. TechNadu, Darksiders publisher THQ Nordic named on DireWolf ransomware leak site (31 August 2026).

<https://www.technadu.com/darksiders-publisher-thq-nordic-named-on-direwolf-ransomware-leak-site/634361/>

21. LevelBlue / Trustwave SpiderLabs, Dire Wolf strikes: new ransomware group targeting global sectors (24 June 2025).

<https://www.levelblue.com/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors>

22. AhnLab ASEC, Dire Wolf ransomware: threat combining data encryption and leak extortion (1 September 2025).

<https://asec.ahnlab.com/en/89944/>

23. MyBroadband, Police emergency number 10111 offline for South African city with 5 million people (2 September 2026). <https://mybroadband.co.za/news/telecoms/665754-police-emergency-number-offline-for-south-african-city-with-5-million-people-as-10111-goes-dow>

n.html

24. Furniture Bargaining Council, Preliminary cybersecurity notification, circular 11-26 (24 August 2026), rechecked 6 September 2026.
<https://fbcweb.furnbed.co.za/>

25. MyBroadband, Largest parcel courier company in South Africa allegedly hit by cyberattack (18 August 2026).
<https://mybroadband.co.za/news/security/662853-largest-parcel-courier-company-in-south-africa-allegedly-hit-by-cyberattack.html>

26. Babcock Africa, news index carrying the Babcock Africa update of 18 August 2026, rechecked 6 September 2026.
<https://www.babcock.co.za/news/>

27. MyBroadband, Toyota South Africa sends warning about SMSs from its official line (12 August 2026).
<https://mybroadband.co.za/news/security/662187-toyota-south-africa-sends-warning-about-smss-from-its-official-line.html>

4. THREAT ACTORS

Two profiles. DireWolf is new to South Africa and is the only group to name a South African target inside the window, so it gets the detailed treatment. MedusaLocker returns because it now sits behind two South African claims in three weeks and because the second of those, Hungry Lion, has technical evidence attached that the first did not.

4.1 DireWolf: A Closed Crew, Windows Only, and Noisy on the Endpoint

DireWolf was first observed in May 2025 and published its first six victims on 26 May 2025.^{21,22} Its own leak-site profile claims financial motivation and a New York base, which no analyst credits. Halcyon assesses it as a closed group of roughly three to seven operators rather than a ransomware-as-a-service operation, with no affiliate recruitment, no infrastructure overlap with other groups and no shared wallets in blockchain analysis, and it is not assessed as a rebrand.²⁸ That matters for a South African defender because there is no affiliate variability to reason about: the tooling that hit one victim is the tooling that hits the next.

The encryptor is Golang, distributed UPX-packed, and Windows only, with no Linux or ESXi variant observed.^{21,28} It checks a mutex named Global\direwolfAppMutex and a marker file at C:\runfinish.exe, and self-deletes if either is present. Encryption is Curve25519 key exchange against a hardcoded attacker public key, with the shared secret run through SHA-256 to derive a ChaCha20 key and nonce; files under 1 MB are fully encrypted and larger files have only their first megabyte encrypted. Files gain the .direwolf extension and every folder gets a note named HowToRecoveryFiles.txt containing a room identifier and per-victim credentials for a negotiation panel. The aggregator's own ransom-note feed independently records HowToRecoveryFiles as this group's note filename, which is a second source for that one indicator.²⁹ Halcyon puts average exfiltration at about 265 GB, staged through gofile.io, with a 30-day publication deadline; the Cartrack claim of 100 GB sits below that average.²⁸

Two behaviours make this group unusually detectable if anyone is watching. It terminates a hardcoded list of 75 services and 59 processes, covering Veeam, BackupExec, MSSQL, Exchange, VMware and several endpoint products, and it disables each service afterwards rather than merely stopping it. And it kills the Windows event log service in an infinite loop, resolving the process identifier through WMI and issuing taskkill repeatedly, so logging stays down even if the service restarts.²¹ A sudden and sustained absence of event log data on a Windows host is therefore a DireWolf signal in its own right, and it is one that does not depend on having a hash.

The gap in the picture is initial access. LevelBlue states plainly that no initial access, reconnaissance or lateral movement technique used by this group is known, and Halcyon calls it a critical intelligence gap, listing spear-phishing, exposed remote access, credential abuse and third-party compromise as suspected only.^{21,28} No CVE has been attributed to DireWolf. One figure should be read with care: Halcyon's victimology, at 41 or more victims across 13 or more countries with about 60 per cent in Asia-Pacific, is dated November 2025 and has been overtaken. The aggregator's group index recorded 125 DireWolf victims when retrieved on 6 September 2026 against 115 a week earlier, so the group added ten listings across the two collections and Cartrack was one of them.³⁰ That is a busy week for DireWolf, and this report draws no South African campaign inference from a single listing. The Asia-Pacific concentration should not be read as current, and no replacement country breakdown is given because none is available in the local collection.

4.2 MedusaLocker: Two South African Claims in Three Weeks

MedusaLocker now sits behind two South African items in three weeks: The Courier Guy on 16 August, which the company denies and which has produced no evidence since, and Hungry Lion, whose leak-site listing surfaced in late August and drew named vendor analysis inside this window.^{13,16} Before The Courier Guy the aggregator held no South African MedusaLocker record at all, so this is a new front against South Africa even though the underlying group is long established. The three Medusa records in the same South African feed belong to a different operation, as set out below.

A disambiguation carried since W35 still applies, because it keeps being got wrong elsewhere. MedusaLocker is not Medusa. They are separate operations, the FBI says so in its own advisory, and the joint advisory applying to MedusaLocker is AA22-181A of 30 June 2022, not the Medusa advisory AA25-071A. What is actionable in the Hungry Lion case is the data class rather than the group profile: the records SOCRadar found are consumer portal credentials harvested by infostealers over nine months, which needs forced rotation, credential-stuffing detection on the customer authentication path and a documented notification assessment. TH-2026-W37-06 covers the detection half.

28. Halcyon, Dire Wolf threat-actor profile (updated 13 November 2025). <https://www.halcyon.ai/threat-group/dire-wolf>

29. ransomware.live, per-group YARA, ransom-note and atomic indicator endpoints, retrieved 6 September 2026. <https://www.ransomware.live/>

30. ransomware.live, group index endpoint /groups, 396 groups, DireWolf recorded at 125 victims on 6 September 2026 against 115 on 30 August 2026. <https://www.ransomware.live/groups>

5. CRITICAL VULNERABILITIES & CISA KEV

Ten vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 31 August and 4 September 2026, against eleven the week before. Five were past their remediation date on Monday 7 September, the day this report was published, all five having carried a 5 September due date from a 2 September listing.⁷ Every due date and overdue count in this section is arithmetic against the locally retrieved catalogue file, catalogVersion 2026.09.04, and every CVSS score is from the NVD feed with its scoring source recorded.^{7,31} All ten carry knownRansomwareCampaignUse of Unknown, which the catalogue uses for most recent entries and which is not the same as no.

The pair that should drive Monday morning is SonicWall SMA 1000. CVE-2026-83548 is a pre-authentication server-side request forgery through an unintended forward proxy, which SonicWall scores 10.0 and NVD confirms at 10.0 under CVSS 3.1; CVE-2026-83549 is a post-authentication OS command injection at 7.8.^{8,31} Taken alone the second looks unremarkable, because it needs an administrator. Rapid7 states that by leveraging the SSRF an attacker could potentially exploit the command injection to execute arbitrary OS commands without prior authentication, which is what makes the pair a single unauthenticated remote code execution problem.⁹ SonicWall's notice is unusually direct about exploitation, saying the vulnerabilities have been confirmed as being actively exploited in the wild, and its remediation instruction goes past patching: contact support for an indicator review, and where indicators are found, re-image or re-deploy the appliance, change all user and administrator passwords and reset TOTP tokens.⁸ Fixed builds are 12.4.3-03526 and 12.5.0-02952, affecting models 6210, 7210 and 8200v. Shadowserver counted at least 420 SMA 1000 appliances reachable from the public internet as at 3 September.³²

Four points of discipline on that pair. No attribution exists: Rapid7 states that no public proof-of-concept, no indicators of compromise and no attribution were identified in the research available at the time of publication.⁹ The INC Ransomware link this report has carried since July belongs to the earlier pair, CVE-2026-15409 and CVE-2026-15410, where Resecurity attributed the chain to an INC affiliate and Volatility attributed zero-day use to UTA0533, and it must not be carried across.³³ The scope is narrower than the vendor name suggests: SonicWall says the new flaws are unrelated to its other products and they do not affect SSL-VPN on SonicWall firewalls or the SMA 100 line.^{8,34} And one widely read account describes CVE-2026-83548 as a command injection stemming from an SSRF weakness; the vendor, Rapid7 and Sophos all place the SSRF at 83548 and the command injection at 83549, and this report follows the vendor.

PaperCut NG and MF entered the catalogue on 31 August with two chained flaws, CVE-2026-81578 and CVE-2026-82078, and the story since is about patch quality rather than severity. The vendor published a bulletin on 27 August and shipped an emergency patch on 28 August, then a second the same day after watchTowr found multiple patch bypasses and a further authentication bypass, and Rapid7's 1 September update states that any organisation running either the first or the second emergency patch is not fully protected and must apply the third.³⁵ Huntress observed exploitation in two customer environments with first activity on 26 August, before the bulletin, and described the observed behaviour as system discovery with no secondary malware or persistence recovered; one intrusion ran for under two minutes.³⁶ PaperCut considers all versions potentially impacted, has patches for versions 24, 25 and 26, and tells customers on version 23 or earlier to upgrade rather than wait.³⁵ A Metasploit module for the chain is public.³⁵ Shadowserver counted more than 1,000 exposed instances.³⁶ No South African figure exists, because the Shodan panel carries no PaperCut product label; that absence is a collection limit, not a finding about South African exposure.

Three of the ten sit on developer and AI infrastructure. Kestra OSS CVE-2026-49869 is a suffix-match bug in AuthenticationFilter: any API path ending in the string configs skips Basic Auth, so an unauthenticated attacker can create and execute a workflow named configs and reach code execution; 10.0, fixed in 1.0.45 and 1.3.21.³⁷ Microsoft assesses with high confidence that initial access in an intrusion it investigated likely occurred through this flaw, with XMRig deployed via a mounted Docker socket. The assessment is likely rather than confirmed, and the advisory's own test environment had no socket mounted, so the outcome is deployment-dependent.³⁸ JFrog Artifactory CVE-2026-82329 is a 9.8 authentication bypass giving administrative access under default configuration, fixed on 28 August across six branches, with

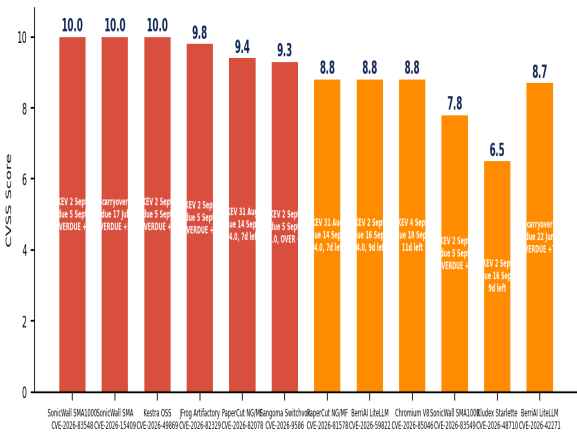
watchTower observing attackers minting administrative tokens and enumerating users, groups and credential sets from a small number of addresses rather than at scale. Patching alone does not close it: JFrog access tokens are independent credentials, so an upgrade does not invalidate a token already minted and revocation is a separate step.³⁹ It is a different flaw from CVE-2026-66384, the 5.3 authenticated path traversal listed on 27 August and carried in the table below; they share fixed branches, so patching for 82329 covers 66384 there but not the reverse.

The LiteLLM and Starlette entries are one problem in two packages. Starlette CVE-2026-48710 is a Host header validation failure that poisons request.url.path, so a request for one path can be made to read as another and path-based authorisation is bypassed; 6.5, fixed in 1.0.1.⁴⁰ LiteLLM CVE-2026-59822 is an MCP authentication bypass in which any bearer token establishes a session, fixed in 1.84.0, with Wiz observing honeypot exploitation using tokens as thin as a single character.^{41,42} The chain that matters was published in June: Horizon3.ai, quoted by The Hacker News, states that CVE-2026-48710 bypasses authentication entirely where a LiteLLM dependency tree includes Starlette 1.0.0 or earlier, turning the June command-injection flaw CVE-2026-42271 into unauthenticated remote code execution rated 10.0 combined.⁴³ Wiz separately reports that external researchers have linked the Qilin ransomware group to exploitation of that chain, and Qilin has South African victims in this report's own feed, which is why the item is carried rather than treated as foreign AI-lab news.⁴²

Sangoma Switchvox CVE-2026-9586 is the entry with the clearest in-window exploitation evidence. Horizon3.ai disclosed an unauthenticated SQL injection at the /pa endpoint, where the PhoneIP field of a posted XML document is concatenated into SQL executed as a PostgreSQL superuser, reaching remote code execution in a single request. Its honeypots recorded a valid exploitation attempt on 30 August 2026, the first day of this window, from 176.65.148.184.¹⁵ Security Risk Advisors independently discovered the same flaw and reported it in May, so the credit is shared. The fix ships in Switchvox 8.4.0.2, build 105309, released 14 July 2026.⁴⁴ Two cautions: Sangoma published this only in release notes, not a security advisory, and the release note's affected-version string conflicts with the version both researchers tested, so the operative fact is the fixed build rather than the affected range. The 9.3 score is CVSS v4.0 per NVD.³¹ Horizon3 counted about 4,000 devices exposed globally, mostly in the United States; no VERIFIED South African figure exists for this product.

Google Chromium V8 CVE-2026-85046 is a type confusion fixed in Chrome 152.0.7977.82 and .83, reported by Salvatore Gulizia on 4 August, with Google stating that it is aware an exploit exists in the wild; Chromium-derived browsers including Edge and Opera shipped the same fix in the first days of September.⁴⁵ It carries no South African exposure figure because it is client software rather than an exposed service, and it needs no hunt: restart the browser fleet.

W37 KEV / CRITICAL CVE SEVERITY | 30 August - 5 September 2026
Ten KEV additions in the window, five already past their remediation date at publication, shown with the two deepest tracked carryovers. CVSS from NVD except CVE-2026-42271, which sits outside this week's NVD extract; scores marked v4.0 in the table are not directly comparable to the v3.1 scores



W37 CISA KEV / Critical CVE Tracking (ten additions 31 August to 4 September plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-83548	SonicWall SMA 1000 Appliances	10.0	SSRF (unauth)	5 Sept	KEV 2 Sept. OVERDUE +2. Vendor confirms active exploitation. Chains to CVE-2026-83549 for unauth RCE (Rapid7). Fixed 12.4.3-03526 / 12.5.0-02952. Re-image if IoCs found. 420 exposed globally (Shadowserver). No SMA-specific ZA figure exists. Ransomware: Unknown. EPSS 0.0071.
CVE-2026-83549	SonicWall SMA 1000 Appliances	7.8	OS command injection (post-auth)	5 Sept	KEV 2 Sept. OVERDUE +2. Reachable without credentials when chained from 83548. Same fixed builds. Ransomware: Unknown. EPSS 0.0163.
CVE-2026-49869	Kestra OSS	10.0	OS command injection (unauth RCE)	5 Sept	KEV 2 Sept. OVERDUE +2. AuthenticationFilter suffix match on '/configs' skips Basic Auth. Fixed 1.0.45 / 1.3.21. Microsoft assesses likely initial access in an XMRig cryptomining intrusion. Ransomware: Unknown. EPSS 0.0192.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-82329	JFrog Artifactory	9.8	Improper authentication (unauth admin)	5 Sept	KEV 2 Sept. OVERDUE +2. watchTowr observed attackers minting admin tokens. Fixed 28 Aug across 7.111.21 / 7.117.28 / 7.125.20 / 7.133.29 / 7.146.38 / 7.161.20. Revoke tokens separately. 2 in ZA. Ransomware: Unknown. EPSS 0.0767.
CVE-2026-82078	PaperCut NG/MF	9.4 (v4.0)	Unsafe reflection (Java bytecode exec)	14 Sept	KEV 31 Aug. Seven days to run. Chains with CVE-2026-81578. Three successive emergency patches; the first two are bypassable. Metasploit module public. More than 1,000 exposed globally. No ZA product label. Ransomware: Unknown. EPSS 0.0169.
CVE-2026-9586	Sangoma Switchvox	9.3 (v4.0)	SQL injection (unauth RCE)	5 Sept	KEV 2 Sept. OVERDUE +2. Unauth /pa endpoint, PhoneIP field, SQL as PostgreSQL superuser. Honeypot exploitation 30 Aug from 176.65.148.184. Fixed 8.4.0.2 build 105309 (14 Jul). ~4,000 exposed globally, mostly US. Ransomware: Unknown. EPSS 0.1185.
CVE-2026-81578	PaperCut NG/MF	8.8 (v4.0)	Missing authentication	14 Sept	KEV 31 Aug. Seven days to run. Auth bypass half of the chain. Huntress observed exploitation from 26 Aug, pre-bulletin. Versions 23 and earlier have no patch; upgrade. Ransomware: Unknown. EPSS 0.0162.
CVE-2026-59822	BerriAI LiteLLM	8.8 (v4.0)	Improper authentication (MCP)	16 Sept	KEV 2 Sept. Nine days to run. Any bearer token establishes an MCP session. Fixed 1.84.0; block /mcp/ at the proxy as a workaround. Wiz observed honeypot exploitation. ZA exposure figure WITHHELD, see 7.2. Ransomware: Unknown. EPSS 0.0087.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-85046	Google Chromium V8	8.8	Type confusion	18 Sept	KEV 4 Sept. Eleven days to run. Google states an exploit exists in the wild. Fixed Chrome 152.0.7977.82/.83; Chromium-derived browsers shipped the same fix in early September. Client software, no exposure figure. Ransomware: Unknown. EPSS 0.0089.
CVE-2026-48710	Kludex Starlette	6.5	HTTP request smuggling	16 Sept	KEV 2 Sept. Nine days to run. Host header poisons request.url.path, bypassing path-based authorisation. Fixed 1.0.1. Chains with LiteLLM CVE-2026-42271 for unauth RCE (Horizon3, combined 10.0); Qilin linked by external researchers. Ransomware: Unknown. EPSS 0.3626.
CVE-2026-42271	BerriAI LiteLLM	8.7	Command injection (MCP preview endpoints)	22 Jun	Carryover, corrected into the table this week. OVERDUE +77, the deepest tracked. Fixed 1.83.7, so moving to 1.84.0 for CVE-2026-59822 also clears it. Chains with Starlette CVE-2026-48710 for unauthenticated RCE. Score as reported by The Hacker News; the entry sits outside this week's NVD extract, so it is not an NVD-confirmed figure.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	Carryover. OVERDUE +52. CVE-2026-15410 shares the listing date, the 17 July due date, the +52 and the KNOWN ransomware flag. Resecurity ties the chain to an INC Ransomware affiliate; Volexity attributes zero-day use to UTA0533. Rebuild rather than patch.
CVE-2026-55040	Microsoft SharePoint	9.1	Weak authentication (JWT forgery)	21 Aug	Carryover. OVERDUE +17. Unchanged since W36: VulnCheck's chain with CVE-2026-63520 itself not a catalogue entry, reaches unauthenticated RCE. Fixed by the July 2026 update. 745 in ZA. EPSS 0.3965, the highest in this table.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-66384	JFrog Artifactory	5.3	Path traversal (authenticated)	10 Sept	Carryover. Three days to run. Distinct from CVE-2026-82329 above; shares fixed branches 7.146.38 and 7.161.20, so the 82329 fix covers it there. 2 in ZA. EPSS 0.0058.

Pattern note: this week's set divides by who is telling you it is exploited. Four sources of come with named responder or vendor evidence a defender can act on, and between them cover six of the ten entries: SonicWall's own confirmation for both SMA 1000 flaws, Huntress on both PaperCut flaws before the vendor bulletin, watchTowr on Artifactory token minting and Horizon3's honeypot catching a Switchvox attempt on 30 August. Three entries come with the catalogue listing and little else: Kestra rests on a Microsoft assessment framed as likely, LiteLLM and Starlette on honeypot probing and a three-month-old chain write-up, and none has a published host count or a named victim. The tenth, Chromium V8, rests on Google's own statement that an exploit exists in the wild. That difference should change what you do with them rather than whether you patch them. Where a responder has published behaviour, hunt for it; where only the catalogue asserts exploitation, patch on the deadline and do not spend analyst hours chasing an indicator nobody has published. Two carryovers outrank most of the additions: SonicWall SMA CVE-2026-15409 and CVE-2026-15410 at fifty-two days overdue with ransomware use recorded as KNOWN, and SharePoint CVE-2026-55040 at seventeen days against 745 exposed South African instances. A third is corrected into the table this week: LiteLLM CVE-2026-42271, the command-injection half of the chain described above, entered the catalogue on 8 June with a 22 June due date and is seventy-seven days overdue, which makes it the deepest item this report tracks rather than the SonicWall pair.⁷ On EPSS, SharePoint scores 0.3965 and Starlette 0.3626 while the vendor-confirmed SonicWall SSRF scores 0.0071; EPSS predicts the next thirty days and lags confirmed activity, so it ranks items not yet in the catalogue and must never deprioritise one that is.⁴⁶

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

32. Cybernews, CISA flags SonicWall SMA 1000 zero-day vulnerability, carrying the Shadowserver count (3 September 2026). <https://cybernews.com/security/cisa-flags-sonicwall-sma-1000-zero-day-vulnerability/>

33. BleepingComputer, CISA: SonicWall SMA1000 flaws now exploited by ransomware gangs (10 August 2026). <https://www.bleepingcomputer.com/news/security/cisa-sonicwall-sma1000-flaws-now-exploited-by-ransomware-gangs/>

34. BleepingComputer, SonicWall warns of actively exploited SMA1000 zero-day flaws (2 September 2026). <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-actively-exploited-sma1000-zero-day-flaws/>

35. Rapid7, PaperCut NG/MF critical zero-day exploited in the wild (28 August 2026, updated 1 September 2026). <https://www.rapid7.com/blog/post/etr-papercut-ng-mf-critical-zero-day-exploited-in-the-wild/>

36. SecurityWeek, PaperCut exploitation escalates to active intrusions (1 September 2026). <https://www.securityweek.com/papercut-exploitation-escalates-to-active-intrusions/>

37. Kestra, GHSA-5vc5-wxxq-3fjx, unauthenticated RCE via authentication bypass in AuthenticationFilter (3 June 2026). <https://github.com/kestra-io/kestra/security/advisories/GHSA-5vc5-wxxq-3fjx>

38. Microsoft Security, When AI infrastructure becomes the target (26 August 2026). <https://www.microsoft.com/en-us/security/blog/2026/08/26/when-ai-infrastructure-becomes-target-securing-gateways-control-points/>

39. BleepingComputer, Hackers exploit critical JFrog Artifactory flaw to forge admin tokens (2 September 2026). <https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-jfrog-artifactory-flaw-to-forge-admin-tokens/>

40. GitHub Advisory Database, GHSA-86qp-5c8j-p5mr, Starlette missing Host header validation (21 May 2026). <https://github.com/advisories/GHSA-86qp-5c8j-p5mr>

41. BerriAI LiteLLM, GHSA-7488-6r32-c95q, MCP authentication bypass via OAuth2 passthrough fallback (30 June 2026). <https://github.com/BerriAI/liteLLM/security/advisories/GHSA-7488-6r32-c95q>

42. Wiz Threat Research, Inside 90 days of attacks on AI infrastructure (27 August 2026). <https://www.wiz.io/blog/ai-infrastructure-honeypot>

43. The Hacker News, LiteLLM flaw CVE-2026-42271 exploited in the wild, chains to unauthenticated RCE, quoting Horizon3.ai (9 June 2026). <https://thehackernews.com/2026/06/litellm-flaw-cve-2026-42271-exploited.html>

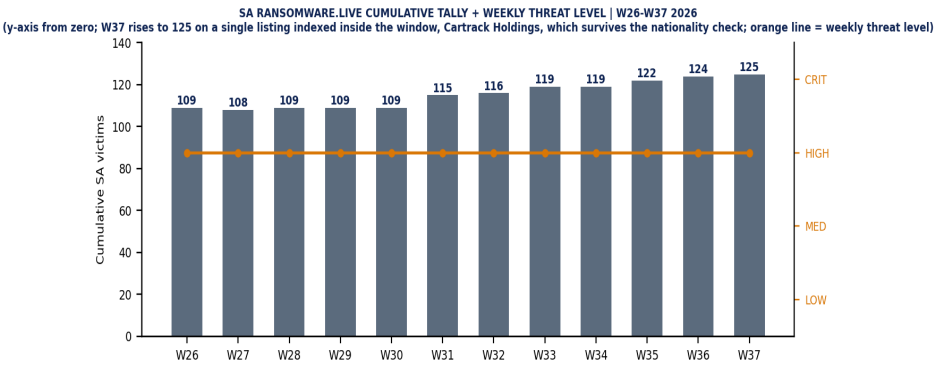
44. Sangoma, Switchvox release notes version 8.4.0.2, build 105309 (14 July 2026). <https://sangomakb.atlassian.net/wiki/spaces/Switchvox/pages/1802371073/Switchvox+-+Release+Notes+Version+8.4.0.2+July+14+2026>

45. Google, Chrome Releases: stable channel update for desktop (3 September 2026). https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html

46. FIRST, Exploit Prediction Scoring System scores, retrieved 6 September 2026. <https://www.first.org/epss/>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 125 records when retrieved at 05:00 UTC on 6 September 2026, up one on the previous week. The collection is country-scoped by path, all 125 records are tagged ZA on a manual count of the file, and the run log records a clean exit.¹³ The single increase is Cartrack Holdings, discovered inside the window on 2 September, and it survives the nationality check: Cartrack is a South African business on a .co.za domain, wholly owned by Karooooo Limited. So the derived count and the feed movement agree at one of one, and no delistings or back-filled listings occurred. A set-difference against the previous week's file confirms one addition and zero removals.



Baseline at W36 close	124 records
New listings dated inside the window	1 (Cartrack Holdings, DireWolf, discovered 2 September 2026 17:53 UTC)
Delistings or restorations	None. Set difference against the 30 August file returns one addition and zero removals
End count at W37 retrieval	125 records, filter purity 1.0 on a manual count of the file
Nationality check	1 of 1 surviving. Cartrack Holdings is South African
Groups active against SA, rolling 120 days	14 by discovery date, composition changed rather than the total: DireWolf enters, PrinzEugen and Stormous age out of the window. The rolling boundary moves each week, so this figure is not a trend
Threat-level drivers	One confirmed utility intrusion outside the leak-site channel entirely, one unsupported extortion claim, five overdue catalogue additions including a vendor-confirmed edge-appliance chain

Two group notes. DireWolf is new to South Africa and is profiled in Section 4.1. Krybit is now silent for a fourth consecutive window: the W35 reading was that the early-August burst of three South African listings in six days was one affiliate's scheduling rather than a country campaign, and a fourth silent window is consistent with that without proving it. The observation that would overturn it is a new South African Krybit listing.¹³

One measurement caution carried from prior editions and still binding. The victim feed is the free v2 tier and is delayed relative to the paid tier, so a listing dated inside this window may have been posted earlier, and one posted late on Saturday 5 September may not appear until next week's collection. The window closes at the end of Saturday precisely because an earlier edition ran to Sunday midnight and missed two South African victims in the unobserved hours. A leak-site listing is also not a breach: of the last ten South African listings this report has carried, one has been confirmed by the organisation named.

7. OSINT EXPOSURE & ATTACK SURFACE

7.1 What the Panel Publishes, and What It Cannot

Every figure in this section is an exposure count: how many instances of a product Shodan sees on the South African internet, not a count of vulnerable systems. The vuln: filter is unavailable on this collection's plan, so no figure here should be read as the number of South African systems affected by a given CVE. Only results the collection marks VERIFIED are published, which means the product facet corroborates the query rather than that anyone has confirmed a version. Two standing queries remain unpublishable: a Palo Alto GlobalProtect title match that disagrees with free text by four orders of magnitude, and an Arista VeloCloud zero returned by two methods that have both failed elsewhere, so the zero is held rather than reported as an absence.⁴⁷ No organisation is named anywhere in this section: the org facet identifies South African companies running exposed appliances, and publishing it in a document distributed without restriction would be targeting information.

7.2 A Figure Withheld: 4,041 LiteLLM Instances

The LiteLLM catalogue addition auto-promoted a new query into the panel, and it returned 4,041 internet-facing LiteLLM instances in South Africa with a product facet 100 per cent on that family. The collection therefore marked it VERIFIED and publishable. It is not published, and the reason is worth setting out because it is a limit of the method rather than a one-off.⁴⁷

The VERIFIED flag tests facet purity: it asks whether the results Shodan returned are all the product the query asked for. It does not test whether the magnitude is credible. Three observations say this one is not. LiteLLM is a proxy layer in front of language models, a narrower category than the general-purpose software populating the rest of the panel, and 4,041 would put it above Apache Tomcat at 929 and about 35 per cent above Fortinet FortiGate at 2,988 in the same country. Censys, in the preview of its 2026 State of the Internet work, identified more than 294,000 distinct public addresses exposing any one of 43 AI and language-model tools worldwide, so 4,041 in one mid-sized country would be about 1.4 per cent of the entire global exposed AI surface across all of them, for a single niche proxy.⁴⁸ And in the best country-level study available, SentinelOne and Censys examining 175,000 Ollama hosts across 130 countries, South

Africa does not appear in the published breakdown at all, for the most widely exposed AI product on the internet.⁴⁹

There is a documented mechanism for exactly this failure. Independent measurement work in May 2026 found a twentyfold spread in host counts for the same population depending on how the question was asked, with a naive banner search returning about 1,165 Ollama hosts where a structured product classification on the same data returned 25,488.⁵⁰ That is the failure mode to rule out before publishing a number of this size, and this collection cannot rule it out from here.

No published global or per-country LiteLLM exposure figure exists, so nothing corroborates or refutes 4,041 directly. That is precisely why it is held. Two observations would settle it, and both are set out in Next-Week Watch: a re-derivation using a structured product classification against a second geolocation source, and whether the figure is stable across the next two collections. A number that moves by an order of magnitude between collections is an artefact; one that holds is a finding. In the meantime the LiteLLM catalogue entry is still a real problem and Section 5 treats it as one. The action does not depend on the count.

7.3 The Standing Exposure Panel

Microsoft SharePoint on-prem	745. Component match, all fingerprinted as Microsoft IIS httpd. The population sitting against the CVE-2026-55040 chain in Section 5, seventeen days overdue
SonicWall, all products	2,975, summing five product strings because Shodan rejects an OR of product filters. It CANNOT be narrowed to the SMA 1000 line that carries this week's two catalogue entries
SonicWall SSL-VPN endpoints	12 on the exact SSL-VPN http proxy product string, the closest available proxy for the SMA line. It cannot separate SMA 1000 from SMA 100 or the older SRA, so it is not an SMA 1000 count
Fortinet FortiGate	2,988. Facet resolves cleanly across model variants and free-text 'fortigate' independently corroborates
Apache Tomcat / Cisco ASA WebVPN	929 across the Tomcat and Coyote JSP engine labels; 391 ASA WebVPN matched on the /+CSCOE+/ path
Exposed RDP and port 445	7,947 services on port 3389, the bulk carrying the Remote Desktop Protocol label; 5,237 on port 445, mostly unfingerprinted, so read the second as services on that port rather than identified SMB servers
WordPress / Citrix Netscaler / Langflow	397, a floor because component detection undercounts; 97, noting Shodan's lowercase spelling of Netscaler; 80, carried
Metabase / MLflow / Ray / vCenter	134, 100, 65 and 3, carried. MLflow and Ray default to unauthenticated administrative APIs; the vCenter figure is an external count of a normally internal system and so a floor
ownCloud / Gitea / Artifactory	87, 8 and 2, carried from last week's additions. Artifactory is the only one of this week's ten additions with a published South African figure
LiteLLM	WITHHELD. See 7.2

These are point-in-time magnitudes. The collection records that Shodan rescan artefacts have moved individual counts by as much as 73 per cent inside twenty-four hours, so week-on-week movement in these figures is not a finding and none is drawn here.⁴⁷ The right use of them is the absolute size of an

exposed population sitting against an actively exploited flaw, which this week is the 745 SharePoint instances against a chain that reaches remote code execution and is seventeen days overdue. For the two SonicWall entries that lead Section 5, there is no honest South African number at all, and the recommendation in Section 1 is written without one rather than substituting the family total.

47. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 05:01 UTC 6 September 2026.

<https://www.shodan.io/search?query=country%3AZA>

48. eSecurity Planet, Censys finds AI and LLM tool exposures up more than 60 per cent (23 July 2026).

<https://www.esecurityplanet.com/threats/censys-finds-ai-llm-tool-exposures-up-more-than-60/>

49. SecurityWeek, 175,000 exposed Ollama hosts could enable LLM abuse (30 January 2026).

<https://www.securityweek.com/175000-exposed-ollama-hosts-could-enable-llm-abuse/>

50. CyberDesserts, AI infrastructure scanning research (14 May 2026).

<https://blog.cyberdesserts.com/ai-infrastructure-scanning-research/>

8. REGULATORY & POLICY

8.1 The Regulator Speaks, and Still Does Not Publish

The Information Regulator held the briefing this report flagged as a W37 watch item, on Monday 31 August 2026 at its Woodmead headquarters, and it produced the most useful number South African breach reporting has had: more than 8,000 security compromise notifications to date, of which 1,220 arrived since the 2026/27 financial year began in April. Chairperson Advocate Pansy Tlakula said that trajectory points to more than 3,000 for the year and, asked directly, called the position very alarming, adding that the Regulator is not sure whether public and private bodies are as alarmed as it is. Advocate Tshepo Boikanyo, the executive for POPIA, attributed what assessments find to inadequate security controls, employee negligence and human error, weak passwords, malware, ransomware and phishing, and said the public sector may not be putting as much effort into protection as the private sector.³

The enforcement content was substantial. An enforcement notice was issued against the South African Bureau of Standards following its 2024 ransomware attack, requiring it within 90 days of receipt to revise policies, conduct personal information impact assessments and implement security measures. The framing matters for any board reading this: the Regulator emphasised that the action was taken because an own-initiated assessment found compliance failures across several POPIA conditions, including excessive processing, inadequate consent mechanisms and insufficient safeguards, and not because SABS was the victim of a cyberattack.^{3,4} What the assessment turns up afterwards is what carries the finding. Two direct-marketing matters, involving OUTsurance and MTN, went to the Enforcement Committee on section 69 and unsolicited electronic communications, from more than 3,800 complaints in the past year of which about ten per cent concerned direct marketing.³ The Regulator has applied for leave to appeal directly to the Supreme Court of Appeal in the Department of Basic Education matter after the High Court refused leave, and it disclosed two Madlanga Commission referrals: a February 2026 referral concerning a former eThekweni city manager, on which its own investigation is complete and the matter has gone to the Enforcement Committee, and a further referral dated 4 August 2026.⁴

The watch item resolves against the Regulator. The test set last week was whether the briefing produced a substantive instrument or announced intentions. Checked on 6 September, the enforcement-notices register carries nothing later than 16 April 2025, so the SABS notice was described at a press conference and is not on the public register, and no media statement, assessment report or guidance note was

published on or after 31 August.⁶ One point of honesty about the test. An enforcement notice was issued inside the window, so on an issuance reading the item resolves in the Regulator's favour. This report reads the test as publication, because the metric measures what a peer organisation can read and learn from, and the narrowing is stated here rather than left to pass unremarked. Every fact in this subsection is journalist-mediated, and the KPI moves to thirteen weeks from the Gauteng Department of Health notice of 8 June 2026 rather than resetting.⁵ One caveat holds, as it has since June: notifications reach the Regulator through an eServices portal it does not routinely publish, so public silence is not evidence that nothing was filed. The 8,000 figure proves that, and is also the argument for publishing something derived from it.

On penalties, the Regulator was candid about why the numbers are small. Tlakula told the briefing that the weakness in POPIA is the grace period: once a body complies within the window, the fine cannot proceed. The fines on the table are R5 million each against the Department of Justice and the Department of Basic Education, both contested, R100,000 each against the IEC and Lancet Laboratories, both paid, R500,000 against Blouberg Local Municipality reduced by a court to R250,000 as a first offence, and R100,000 against FT Rams Consulting.⁵¹ The Regulator intends to propose amendments to Parliament, including immediate fines on a finding of non-compliance in place of the grace period, and for PAIA both administrative fines equivalent to POPIA's and a power to release information directly after 180 days of non-compliance. On PAIA compliance itself, 417 of 853 public bodies filed between 1 April and 18 August 2026, about 49 per cent, and only 91 of 257 municipalities.⁴ One source-quality note: that briefing states the public-body rate as approximately 9 per cent in one place and approximately 49 per cent in another; 417 of 853 is 48.9 per cent, so 49 is used here. A broader list of live investigations reported by one outlet is single-sourced and is not carried.

8.2 A 24-Hour Clock for Financial Institutions, Live Since 1 September

The change with the most direct operational consequence this week affects every regulated financial institution in the country and took effect inside the window. Under FSCA and Prudential Authority Joint Communication 5 of 2026, with the requirements in Joint Notice 2 of 2026, an institution that classifies an information technology or cyber incident as material must give initial notification within 24 hours, provide an update within 14 calendar days, and deliver a final investigation report within a period agreed with the responsible authority.⁵² Three details decide whether an incident response plan actually complies. The 24 hours are ordinary hours, not business hours, so the clock runs over weekends and public holidays. The authorities declined to prescribe uniform materiality thresholds, so the classification decision, and the moment the clock starts, sit with the institution and need to be written down before an incident rather than argued during one. And outsourcing an IT or cyber function does not transfer the obligation. Banks, mutual banks, insurers and controlling companies submit through the Prudential Authority's Umoja portal; other institutions submit to the FSCA.⁵² This subsection rests on a single secondary source: the underlying Reserve Bank documents could not be retrieved in this environment, and that limitation is recorded in Section 12.

SARS published no new scam alert inside the window, the most recent remaining SARS-SCAM-399 of 27 August, a fake Notice of Assessment ITA34. The absence during filing season is worth a line but is not itself evidence that lure volumes fell.⁵³

On fraud, BusinessTech's write-up of the SABRIC 2025 annual crime statistics landed inside the window although the underlying report was released on 4 August. Credit card account-takeover losses rose 66.7

per cent to about R21 million and debit card account-takeover losses rose from R1.65 million to R7.02 million, with South Africa accounting for 80.1 per cent of credit card and 75.9 per cent of debit card account-takeover losses. Combined card fraud losses rose 18 per cent year on year to R1.75 billion.⁵⁴ Account takeover is the same failure mode as the Hungry Lion credential exposure in Section 3.3, seen from the bank's side.

8.3 Who to Call

Six South African teams are registered with FIRST and remain current in this week's collection: the Cybersecurity Hub for private and public sector organisations, ECS-CSIRT at the State Security Agency for government and military, SA NREN CSIRT for research and education, and the UCT, Standard Bank Group and Vodacom Group teams.⁵⁵ For a state-owned utility in the position Rand Water was in on 3 September, the Cybersecurity Hub is the constituency match and ECS-CSIRT the government one. Full contact details are in the W34 edition. Identify which team covers you before you need it, and note that notifying a CSIRT is not the same as notifying the Information Regulator under POPIA section 22, nor the same as the FSCA and Prudential Authority notification in 8.2; a regulated financial institution suffering a material incident involving personal information now owes all three.

51. ITWeb, POPIA grace period limits regulator's fines (2 September 2026).

<https://www.itweb.co.za/article/popia-grace-period-limits-regulators-fines/P3gQ2qGAIAk7nRD1>

52. Moonstone, New IT and cyber incident reporting template now in effect, reporting FSCA and Prudential Authority Joint Communication 5 of 2026 (3 September 2026).

<https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>

53. SARS, Scams and phishing index, most recent entry SARS-SCAM-399 (27 August 2026), checked 6 September 2026.

<https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>

54. BusinessTech, Warning about bank account takeovers in South Africa, reporting the SABRIC 2025 crime statistics released 4 August 2026 (1 September 2026). <https://businesstech.co.za/news/banking/872833/warning-about-bank-account-takeovers-in-south-africa/>

55. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 6 September 2026, six teams. <https://www.first.org/members/teams/>

9. WEEKLY THREAT HUNT & IOCs

Six missions. Three P1 cover the actor that named a South African organisation this week and the two catalogue entries where the vendor or a named responder confirmed exploitation against internet-facing systems. Two P2 cover the remaining additions with published behaviour to hunt on, and the generic case behind Section 3.1. One P3 covers the consumer credential exposure in Section 3.3, which is the item on this list most likely to be happening in a South African environment already. Indicators come from vendor advisories, named responder reporting and the per-group YARA and ransom-note feeds, and the atomic detail is exported to iocs_w37.csv rather than repeated in full here.²⁹ One catalogue addition carries no mission and the reason is stated: Google Chromium V8 CVE-2026-85046 is client software with no published exploitation detail beyond Google's own statement, so the remedy is a browser fleet restart. PaperCut and Sangoma Switchvox share TH-2026-W37-03 as one pre-authentication application-server problem, and Artifactory, Kestra, LiteLLM and Starlette share TH-2026-W37-04 as one control-plane problem. Two missions continue from W36 with new justification: TH-2026-W37-03 carries PaperCut forward because a third emergency patch has since shipped and Huntress has published pre-bulletin exploitation, and TH-2026-W37-04 carries the exposed developer-server hunt forward because four new catalogue entries landed on that estate. The SharePoint mission run in W35 and W36 is retired: nothing

about CVE-2026-55040 changed this week and the hunt logic is unaltered, while Section 5 keeps it in the table because the exposure and the overdue count still stand. Every TH identifier referenced in Sections 3 and 4 exists in this section.

TH-2026-W37-01: DireWolf: Pre-Encryption Behaviour on Windows Hosts

P1 CRITICAL: SA organisation named 2 September; the group is Windows only and loud on the endpoint

Hypothesis: A DireWolf operator is present on Windows hosts and has begun the pre-encryption sequence, being service and process termination, shadow copy and backup catalogue destruction, event log clearing and staged exfiltration to a file-sharing service, ahead of dropping a Golang ChaCha20 encryptor. The hunt runs whether or not the organisation has been named, because the group's on-host behaviour is fixed: it is a closed crew with no affiliate variation.

MITRE ATT&CK: T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), T1489 (Service Stop), T1562.001 (Impair Defenses: Disable or Modify Tools), T1070.001 (Indicator Removal: Clear Windows Event Logs), T1070.004 (Indicator Removal: File Deletion), T1567 (Exfiltration Over Web Service), T1027 (Obfuscated Files or Information), T1529 (System Shutdown/Reboot).

IOCs: Mutex Global\direwolfAppMutex; marker file C:\runfinish.exe; ransom note HowToRecoveryFiles.txt in every folder, independently recorded as this group's note filename by the aggregator's ransom-note feed; appended extension .direwolf; exfiltration staging to gofile.io; leak site direwolfcdkv5whaz2spehizdg22jsuf5aeje4asmetpbt6ri4jnd4qd[.]onion. Sample hashes and the anti-recovery command set are in iocs_w37.csv.

Data Sources: Sysmon process creation and command line, Windows Security and System event logs, EDR service-control and process-termination telemetry, file creation on C:\ root, and egress netflow or proxy logs.

Detection Guidance: The highest-value detection needs no hash. Alert on repeated termination of the event log service, because this group resolves the eventlog process identifier through WMI and issues taskkill in a loop so logging stays down through restarts; a sustained gap in event log data on an otherwise live host is the signal. Alert on the anti-recovery command set as a burst rather than individually: vssadmin delete shadows, wmic shadowcopy delete, four wbadmin invocations, two bcdedit recovery settings and four wevtutil cl calls inside a short window. Alert on sc config with start= disabled across many services. Watch for creation of C:\runfinish.exe, and note that it and the mutex act as a kill switch: their presence makes the sample self-delete.

TH-2026-W37-02: SonicWall SMA 1000: SSRF to Unauthenticated Command Execution**P1 CRITICAL:** vendor confirms active exploitation; 2 days overdue at publication; a July pair 52 days overdue

Hypothesis: An attacker has used CVE-2026-83548, a pre-authentication server-side request forgery through an unintended forward proxy, to reach internal functionality on an SMA 1000 appliance and then CVE-2026-83549 to execute operating system commands without ever authenticating. Where the appliance also still carries the July pair, assume a longer dwell.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1059 (Command and Scripting Interpreter), T1078 (Valid Accounts), T1552 (Unsecured Credentials), T1556 (Modify Authentication Process).

IOCs: No public proof-of-concept, indicators of compromise or attribution had been published at the time of writing; Rapid7 states this explicitly. Do not fabricate indicators. The actionable artefacts are version strings: affected platform hotfix 12.4.3-03453 and 12.5.0-02835, fixed 12.4.3-03526 and 12.5.0-02952, on models 6210, 7210 and 8200v. For the carryover chain, Volexity's UTA0533 malware names KNUCKLEBALL, Sou5, ROOTRUN and ORANGETAIL are the published set.

Data Sources: SMA 1000 appliance and Work Place logs, management-interface access logs, outbound connections originating from the appliance itself, VPN authentication records, and TOTP enrolment or reset events.

Detection Guidance: Treat outbound connections initiated by the appliance to arbitrary hosts as the core SSRF signal, since a VPN concentrator originates traffic to a small and predictable set of destinations. Contact SonicWall Support for the indicator review the vendor asks for; where indicators are found the vendor's own instruction is to re-image or re-deploy, change all user and administrator passwords and reset TOTP tokens, so plan for rebuild rather than patch. Where CVE-2026-15409 or CVE-2026-15410 was never remediated, rebuild regardless: fifty-two days of reachability means the credential and TOTP seed material should be treated as attacker-known.

TH-2026-W37-03: Pre-Auth Code Execution on Application Servers: PaperCut and Sangoma Switchvox**P1 CRITICAL:** PaperCut exploited before the vendor bulletin; a Switchvox attempt caught on 30 August

Hypothesis: An attacker has reached operating system command execution on an internet-facing application server without credentials. On PaperCut, by posting to the Apache Tapestry complex-direct request handler to execute a component on a page other than the one displayed, rewriting user-lookup database settings and then triggering a user search that drives a Derby to H2 JDBC chain into the bundled Nashorn engine; organisations on only the first or second emergency patch are still exploitable. On Switchvox, by posting XML to the unauthenticated /pa endpoint so that the PhoneIP field is concatenated into SQL executed as a PostgreSQL superuser.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1505 (Server Software Component), T1005 (Data from Local System), T1070 (Indicator Removal).

IOCs: PaperCut: POST requests to /app?service=direct/1/Error/ConfigEditor/quickFindForm, /app?service=direct/1/Error/ConfigEditor/\$Form and /app?service=direct/1/Error/UserList/\$QuickFind.\$Form; modification of the configuration keys user-lookup.db-driver, user-lookup.db-url, user-lookup.id-to-username-sql and user-lookup.enabled; log strings 'ERROR No suitable driver found for jdbc:no:x' and 'ERROR DatabaseUtils - Database error looking up cardID: VALUES CAST'; child processes spawned by pc-app.exe; missing or truncated server.log. Switchvox: POSTs to /pa carrying a PolycomIPPhone XML document, evidence in /var/log/switchvox/db-quirks.log, attacker address 176.65.148.184 with a payload piping netcat output to a shell; fixed in 8.4.0.2 build 105309.

Data Sources: PaperCut server.log and reverse proxy access logs for the /app endpoint, EDR process-creation telemetry with pc-app.exe as parent, configuration change auditing, and for Switchvox the web access logs for /pa plus /var/log/switchvox/db-quirks.log.

Detection Guidance: Alert on any modification of the four user-lookup configuration keys, which in normal operation change during a directory integration project and almost never otherwise, and on any child process of pc-app.exe that is not a known PaperCut helper. Treat a missing or truncated server.log as an incident rather than a housekeeping problem. Confirm which emergency release you are on before closing the ticket: the third is the only complete one. For Switchvox, any unauthenticated POST to /pa from an address outside your handset ranges is worth investigating, since the endpoint exists for phone provisioning; the honeypot attempt on 30 August used a single request, so there is no slow burn to catch.

TH-2026-W37-04: Developer and AI Control Plane: Artifactory, Kestra, LiteLLM and Starlette**P2 HIGH:** four additions on build and AI infrastructure; Artifactory 2 days overdue; Qilin linked to the LiteLLM chain

Hypothesis: An attacker reached a control-plane service that was never meant to be internet-facing, either by forging an Artifactory administrative token, or through the Kestra authentication-filter suffix match, or through the LiteLLM MCP bearer-token bypass, or through the Starlette Host-header path poisoning that defeats path-based authorisation in front of the last two, and used it to enumerate credentials, mine cryptocurrency or reach the surrounding container estate.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1528 (Steal Application Access Token), T1087 (Account Discovery), T1195.002 (Compromise Software Supply Chain), T1496 (Resource Hijacking), T1610 (Deploy Container), T1611 (Escape to Host), T1552 (Unsecured Credentials).

IOCs: Artifactory: fixed 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38 and 7.161.20, released 28 August 2026; watchTower reports exploitation from a small number of addresses with no broad scanning, and no address list has been published, so none is asserted here. Kestra: requests to any API path ending in the string 'configs', and creation or execution of a flow named configs; fixed 1.0.45 and 1.3.21; cryptomining indicators from Microsoft's investigation are 172.232.38[.]92:32991, auto.c3pool[.]org:443 and 47.86.197[.]116, with XMRig deployed through a mounted Docker socket. LiteLLM: GET /v1/models with an Authorization bearer value as short as a single character, observed by Wiz; fixed 1.84.0, with blocking /mcp/ at the reverse proxy as the interim control. Starlette: a Host header containing a path, such as example.com/abc; fixed 1.0.1.

Data Sources: Artifactory access and token audit logs, reverse proxy logs including the Host header, container runtime and Docker socket auditing, CI/CD job logs, and egress netflow for mining pool destinations.

Detection Guidance: Revoke and rotate Artifactory access tokens as a task separate from the upgrade, because the upgrade does not invalidate a token already minted; start with anything long-lived that has no named owner. Log the Host header if you do not already, since the Starlette bypass is invisible without it, and alert where the reconstructed path disagrees with the routed path. Alert on an MCP session established with a bearer token shorter than your shortest legitimate one, and on administrative API calls from addresses with no prior authentication history. Treat sustained high CPU on a worker node with an outbound connection to a mining pool as an incident. Note the Kestra deployment dependency: Microsoft's intrusion involved a mounted Docker socket, so unmounting it is a control in itself.

TH-2026-W37-05: Destructive Intent Against an IT Estate Adjacent to Operational Technology

P2 HIGH: confirmed intrusion and server damage at a bulk water utility; FBI and CISA sector alerts, July 2026

Hypothesis: An intruder is inside the corporate IT estate of a utility, municipality or industrial operator, is damaging or destroying systems rather than encrypting them for payment, and may be probing towards the operational technology boundary. This mission is written generically because no indicator has been published for the Rand Water intrusion and none is invented here.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1133 (External Remote Services), T1021 (Remote Services), T1485 (Data Destruction), T1561 (Disk Wipe), T1489 (Service Stop), T0886 (ICS: Remote Services), T0812 (ICS: Default Credentials).

IOCs: No actor indicators exist for the South African incident. The published sector context is the FBI alert of July 2026 on actors targeting internet-facing programmable logic controllers in the water and wastewater sector, and CISA's matching alert of 30 July 2026. The artefacts to hunt are the generic destructive set: mass file deletion or overwrite, disk or volume operations outside a maintenance window, and service or scheduled-task destruction across multiple hosts.

Data Sources: Domain controller and file server audit logs, backup job history, EDR telemetry for destructive commands, jump-host session records, and netflow across the IT to OT boundary.

Detection Guidance: Alert on out-of-hours activity touching many hosts, since the intrusion in Section 3.1 was identified at night. Test the assumption that the boundary holds rather than asserting it: enumerate every path from the corporate domain into the control network, including engineering workstations, vendor remote access and historian replication, and confirm each is authenticated and logged. Verify that the disaster recovery environment can run the business and that its restore path cannot be reached with production credentials.

TH-2026-W37-06: Consumer Portal Account Takeover From Infostealer Logs

P3 MEDIUM: nine months of SA quick-service restaurant customer credentials in stealer logs

Hypothesis: Credentials for your customer-facing self-service portal are circulating in infostealer logs harvested from customers' own infected devices, and are being replayed against your authentication endpoint. This is not a network intrusion and will not appear in intrusion telemetry.

MITRE ATT&CK: T1555 (Credentials from Password Stores), T1110.004 (Credential Stuffing), T1078 (Valid Accounts), T1589.001 (Gather Victim Identity Information: Credentials).

IOCs: No hashes apply. The artefact to look for is records tied to your own domain in stealer-log corpora, as SOCRadar found for hungrylion.co.za with 23 records dated October 2025 to July 2026. Detection indicators are behavioural: authentication attempts spread across many accounts from few addresses, low per-account attempt counts, a success ratio out of line with your normal failed-login rate, and successful logins from device fingerprints with no history for that account.

Data Sources: Customer authentication logs, web application firewall and bot-management telemetry, device fingerprinting, password-reset events, and any stealer-log monitoring you subscribe to.

Detection Guidance: Measure your baseline first, because credential stuffing shows up mainly as a change in the ratio of successful to failed logins and you need the ratio before you need the alert. Force rotation for accounts appearing in a stealer corpus rather than waiting for misuse, since the credential is already valid. Where takeover is confirmed, write down the POPIA section 22 assessment while the investigation runs, noting the Regulator's position this week that a compromise should be reported as soon as one is reasonably sure it has occurred rather than once it is confirmed.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. Work the five overdue catalogue additions on Monday 7 September. All five carried a 5 September due date: SonicWall SMA 1000 CVE-2026-83548 and CVE-2026-83549, Kestra OSS CVE-2026-49869, JFrog Artifactory CVE-2026-82329 and Sangoma Switchvox CVE-2026-9586. The five with time to run are the two PaperCut flaws on 14 September, LiteLLM and Starlette on 16 September and Chromium V8 on 18 September. Fixed versions are in the Section 5 table. Where any of these faces the internet, take it off the internet while you patch: Artifactory, Kestra and LiteLLM are control-plane systems with no business being publicly reachable at all.

2. Rebuild SonicWall SMA 1000 appliances rather than patching them, where indicators are found. The vendor's own remediation is an indicator review through SonicWall Support, then re-image or re-deploy, change every user and administrator password, and reset TOTP tokens. Where the July pair was never remediated, skip the review and rebuild: fifty-two days of reachability on an appliance holding session and one-time-password material is long enough to assume the credential store is known to the attacker. Run TH-2026-W37-02 against appliance-originated outbound connections either way.

3. Confirm which PaperCut emergency patch you are running. Three out-of-band releases shipped in quick succession because the first two were bypassed, and only the third is complete. Versions 23 and earlier have no patch and need an upgrade. Then run TH-2026-W37-03 against the four user-lookup configuration keys and any child process of pc-app.exe, because exploitation was observed on 26 August, before the vendor bulletin, so a compromise can predate your awareness of the flaw.

4. Revoke Artifactory tokens as a task separate from the upgrade, and log the Host header. Access tokens survive a binary upgrade, so an administrative token minted through CVE-2026-82329 stays valid on a patched instance: enumerate long-lived tokens, revoke anything without a named owner, and rotate the rest. Separately, the Starlette path bypass is invisible unless the Host header is logged, and alerting where the reconstructed path disagrees with the routed path is a one-line reverse proxy change and the cheapest item on this list. While you are in the LiteLLM estate, note the correction in Section 5: CVE-2026-42271 has been overdue since 22 June, and the upgrade to 1.84.0 clears it too.

5. Test the IT to OT boundary rather than asserting it. The Rand Water incident is being read by outside specialists as evidence that segmentation held, and that reading is only useful to you if you have enumerated every path from your corporate domain into a control network: engineering workstations, vendor remote access, historian replication and backup infrastructure. Confirm each is authenticated and logged, and confirm your disaster recovery environment can run the business and cannot be reached with production credentials.

Management (CISO / Board)

1. Assume your sector's incident history is invisible to you, and stop reasoning from its absence. The Information Regulator holds more than 8,000 breach notifications and publishes none of them; a JSE-listed miner disclosed a breach in audited statements that a journalist could not find on the

Regulator's website; the country's largest bulk water utility told the market only because it has listed debt. Three disclosure regimes, and none produces peer-learning material. Any assurance argument resting on your sector looking quiet is resting on nothing.

2. Write down your materiality threshold before you need it, if you are a regulated financial institution.

The FSCA and Prudential Authority notification template took effect on 1 September 2026 with a 24-hour initial notification clock that runs in ordinary hours, over weekends and public holidays. The authorities deliberately did not prescribe materiality thresholds, so the decision that starts the clock is yours: make it calmly in advance and have it approved. Outsourcing the function does not transfer the obligation.

3. Note what the SABS enforcement notice was actually for. The Regulator was explicit that it acted because an own-initiated assessment after the attack found compliance failures across several POPIA conditions, including excessive processing and inadequate consent mechanisms, and not because SABS was attacked. The board question that follows is worth asking now: if the Regulator assessed us tomorrow, what would it find about how we collect and retain personal information, independently of how we were breached.

4. Put a stated hour count into supplier notification clauses at the next three renewals. Rand Water's disclosure trigger was its bondholders. Most of your suppliers have no trigger at all, and POPIA reaches them only where personal information is involved. A clause with a specific number of hours, an escalation contact and an obligation to notify on suspicion rather than on confirmation is the only mechanism most organisations actually have.

5. Fund the disaster recovery environment as an operating capability. Rand Water is running its business from a recovery site while it replaces equipment, and its own officer said the utility would have been in serious trouble without it. That is the difference between a reportable incident and a public outage affecting 16 million people. Ask when yours was last used to run production work for a full day rather than tested for an hour.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 20th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for a twentieth consecutive week (30 August to 5 September 2026). Escalation to CRITICAL was closer this week than in any recent edition and was still rejected, on the specific ground that the criterion is service impact rather than target prominence: Rand Water's water treatment, quality control and bulk supply operations continued throughout, no systemically important institution went out of service, and no national-scale outage occurred. Had bulk supply been interrupted, or had the intrusion reached the control network, the assessment would be different and the report would say so. De-escalation to MEDIUM was rejected on the first confirmed compromise of South African bulk water infrastructure this series has carried, and on a vendor-confirmed edge-appliance exploitation chain that is already overdue.

Rationale

- **A confirmed intrusion at critical national infrastructure, disclosed by the victim.** Rand Water confirmed to the JSE debt market that its network was breached and that servers were damaged, and it is running from its disaster recovery site while it replaces equipment. No actor is named and no ransomware family is attributed. The operational technology side was not affected, which is the reason this is a HIGH-level event rather than a CRITICAL one.
- **An edge-appliance chain the vendor itself says is being exploited.** SonicWall states that CVE-2026-83548 and CVE-2026-83549 are confirmed as actively exploited and instructs customers with indicators to rebuild rather than patch. Both were overdue at publication. The July SMA 1000 pair, with ransomware use recorded as KNOWN, has now been overdue for fifty-two days, so a South African organisation running that appliance unpatched has been exploitable for the better part of two months.
- **The regulator quantified the problem and published nothing.** More than 8,000 security compromise notifications to date and 1,220 since April is the largest number this report has been able to attach to South African breach volume, and it arrived at a press conference rather than in an instrument. The enforcement register has carried nothing since April 2025. Deterrence that exists only in journalism is weaker than deterrence that exists on a register, and the Regulator's own proposal to remove the POPIA grace period is an acknowledgement of that.
- **One unsupported extortion claim, and a quiet leak-site week otherwise.** A single new South African listing entered the feed, DireWolf against Cartrack Holdings, with 100 GB claimed, no victim statement and no corroboration. One listing is the lowest weekly figure since W34. That is not improvement on its own, because the week's confirmed material arrived entirely outside the leak-site channel, which is the second time in five weeks that has happened.

Next-Week Watch (W38)

- **Rand Water, and whether anything more is disclosed.** Three observations would each move the assessment in a different direction: a named actor or ransomware family, which would turn an unattributed destructive intrusion into a known campaign; a statement that personal information was involved, which would bring POPIA section 22 and the Information Regulator into a matter that so far has not touched them; and a return from Centurion to the primary site, which would indicate the sanitisation is complete. Silence on all three is also informative, since it suggests an investigation still open at day ten.
- **Cartrack and Karooooo.** The claim stays CLAIMED until one of two things happens: Karooooo files a SENS announcement or a NASDAQ disclosure referencing an incident, or DireWolf publishes the 100 GB it says it holds. The group's stated practice is a thirty-day window between listing and full release, which puts the second observation in early October rather than next week. A denial from the company would not settle it either way, as The Courier Guy matter has demonstrated across three editions.
- **Whether the 4,041 LiteLLM figure survives a second method.** This is the report's own measurement problem and it is stated as one. Two observations would separate a genuine population from a collection artefact: a re-derivation using a structured product classification against an independent geolocation source, and stability across the next two collections. An order-of-magnitude move between collections settles it as an artefact. A figure that holds within a few per cent would be a finding and would need an explanation for why South Africa hosts so much of a niche AI proxy. Until then the

count is named only as a withheld figure and is used as a finding nowhere.

- **Whether the SABS enforcement notice reaches the public register.** The Regulator described the notice at a briefing on 31 August. The distinguishing observation is narrow and checkable: does an instrument dated August or September 2026 appear on the enforcement-notices page. If it does, the publication drought resets and the KPI returns to zero. If it does not, the pattern is confirmed as a communications practice rather than a backlog, and this report will say so and stop tracking it weekly.
- **Krybit, now silent for four windows.** The W35 reading, that the early-August burst was one affiliate's scheduling rather than a country campaign, strengthens with each silent window without ever being proved. The distinguishing observation remains simply whether another South African listing appears. If W38 is a fifth silent window this report will retire the item rather than restate it.
- **Whether the developer-server exposure has legs, carried from W36.** Counts held broadly steady: ownCloud 87, Gitea 8, Artifactory 2, MLflow 100, Ray 65. One stable collection is not the two or three the W36 test called for, so the item carries forward unchanged. The Courier Guy, Babcock, Toyota's unnamed SMS provider, the Furniture Bargaining Council exfiltration claim and Rohloff Group all remain CLAIMED or open with no development, and are carried without re-argument.

12. OSINT SOURCES CONSULTED

All sources are TLP:CLEAR and publicly accessible, numbered in order of first citation. Every cited URL was retrieved and confirmed to contain the claim attributed to it, on 6 September 2026. **Collection notes.** The feed run completed at 05:05 UTC on 6 September 2026 and passed its integrity check with a clean exit. The victim feed returned 125 records, all tagged ZA; the run log records filter purity 1.0 and this was confirmed independently by counting the records, because the written file carries no filter_purity field of its own. The catalogue file is catalogVersion 2026.09.04. **A figure withheld.** The Shodan collection returned 4,041 internet-facing LiteLLM instances in South Africa and marked it VERIFIED on facet purity. It is not published, for the reasons in Section 7.2, and the KPI row was renamed to make the distinction between available and published explicit. Two standing queries remain unpublishable, and no Shodan product label exists for PaperCut, Sangoma Switchvox, Kestra or the SMA 1000 line, so no South African figure is given for any of them. **Environment limitations.** cisa.gov returns an empty body here, so every catalogue date and due date comes from the locally retrieved file. Three primary documents could not be retrieved: the Reserve Bank PDFs behind Joint Communication 5 of 2026, the SonicWall PSIRT detail page for SNWLID-2026-0016, which renders as an empty shell, and the PaperCut bulletin of 27 August, which is client-side rendered. The SonicWall product notice was read directly and is the primary source for that advisory; the PaperCut and Reserve Bank items rest on secondary reporting and are flagged as such in the text. Toyota South Africa's own website is client-side rendered and could not be read, so that carryover is phrased as no publicly reported update. **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. **Single-source disclosure.** Four items rest on one publication because no other account could be found: the FSCA and Prudential Authority notification template, carried by Moonstone; the Hungry Lion credential analysis and the Implats disclosure, both carried by ITWeb; and the Cartrack listing, which no outlet has carried and which rests on the aggregator record alone. **Claims deliberately excluded.** No actor, ransomware family, ransom figure or indicator is attributed to the Rand Water incident, because none has been published. The INC Ransomware attribution attached to the July SonicWall SMA pair is not carried across to this week's pair, which has no attribution at all. A broader list of Information Regulator

investigations reported by one outlet is not carried. A widely repeated claim that DireWolf listings include fabricated victims could not be traced to any sourced publication and is not repeated; the sourced version, that recent listings have been published without screenshots or sample files and remain unconfirmed by the named victims, is used instead. Halcyon's Asia-Pacific victim concentration is dated November 2025 and is explicitly not presented as current. No correction to a prior edition was required this week.

1. ITWeb, Hackers breach Rand Water's defences (4 September 2026). <https://www.itweb.co.za/article/hackers-breach-rand-waters-defences/Gb3BwMWaO4ov2k6V>
2. TechCentral, Cyberattack hits South Africa's biggest water utility (3 September 2026). <https://techcentral.co.za/rand-water-cyberattack/285746/>
3. ITWeb, InfoReg concerned by 'alarming' rate of data breaches (31 August 2026). <https://www.itweb.co.za/article/info-reg-concerned-by-alarming-rate-of-data-breaches/rxP3jqBE2ZLMA2ye>
4. Polity / Werksmans Attorneys, The regulator is watching: new enforcement signals for POPIA and PAIA compliance (1 September 2026). <https://www.polity.org.za/article/the-regulator-is-watching-new-enforcement-signals-for-popia-and-paia-compliance-2026-09-01>
5. Information Regulator of South Africa, Gauteng Department of Health enforcement notice, 8 June 2026, the anchor for the weeks-since-publication count. <https://infoeregulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>
6. Information Regulator of South Africa, enforcement notices register, nothing later than 16 April 2025, checked 6 September 2026. <https://infoeregulator.org.za/enforcement-notices/>
7. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.09.04, released 4 September 2026, retrieved 6 September 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
8. SonicWall, Product notice: SMA 1000 series affected by multiple vulnerabilities, SNWLID-2026-0016 (1 September 2026). <https://www.sonicwall.com/support/notices/product-notice-sma-1000-series-affected-by-multiple-vulnerabilities-snwlid-2026-0016/kA1VN000002AXmQ0AW>
9. Rapid7, Critical SonicWall SMA1000 vulnerabilities CVE-2026-83548 and CVE-2026-83549 exploited in the wild (2 September 2026). <https://www.rapid7.com/blog/post/etr-critical-sonicwall-sma1000-vulnerabilities-cve-2026-83548-cve-2026-83549-exploited-in-the-wild/>
10. ransomware.live, victim record: Cartrack Holdings, DireWolf, discovered 2 September 2026. <https://www.ransomware.live/id/Q2FydHJhY2sgSG9sZGluZ3NAZGlyZXdvbGY=>
11. Karooooo Limited, JSE SENS announcements index, most recent entry 28 July 2026, checked 6 September 2026. <https://karooooo.com/jse-sens-announcements/>
12. MyBroadband, R500-million replacement for South Africa's top supercomputer gathering dust (30 August 2026). <https://mybroadband.co.za/news/government/665077-r500-million-replacement-for-south-africas-top-supercomputer-gathering-dust.html>
13. ransomware.live, SA victim records, /v2/countryvictims/ZA, 125 records all tagged ZA, retrieved 05:00 UTC 6 September 2026. <https://www.ransomware.live/>
14. The Citizen, Forget poisoned water, a cyberattack's real threat to SA is empty reservoirs (4 September 2026). <https://www.citizen.co.za/news/forget-poisoned-water-a-cyberattacks-real-threat-to-gauteng-is-empty-reservoirs/>
15. Horizon3.ai, Off the hook: active exploitation of Sangoma Switchvox CVE-2026-9586 (1 September 2026). <https://horizon3.ai/attack-research/disclosures/cve-2026-9586-sangoma-switchvox-rce/>
16. ITWeb, Hungry Lion customer creds online for months (1 September 2026). <https://www.itweb.co.za/article/hungry-lion-customer-creds-online-for-months/6GxRKqYQEDZqb3Wj>
17. MyBroadband, South Africa's largest bulk water utility allegedly crippled by cyberattack (2 September 2026). <https://mybroadband.co.za/news/security/665683-south-africas-largest-bulk-water-utility-crippled-by-cyberattack.html>
18. CISA, Water and wastewater systems sector urged to protect OT against activity targeting PLCs (30 July 2026). <https://www.cisa.gov/news-events/alerts/2026/07/30/cisa-urges-water-and-wastewater-systems-sector-protect-ot-against-activity-targeting-plcs>
19. ITWeb, Implats pushes AI as it addresses cyber breach (3 September 2026). <https://www.itweb.co.za/article/implats-pushes-ai-as-it-addresses-cyber-breach/Gb3BwMWaOwpv2k6V>
20. TechNadu, Darksiders publisher THQ Nordic named on DireWolf ransomware leak site (31 August 2026). <https://www.technadu.com/darksiders-publisher-thq-nordic-named-on-direwolf-ransomware-leak-site/634361/>
21. LevelBlue / Trustwave SpiderLabs, Dire Wolf strikes: new ransomware group targeting global sectors (24 June 2025). <https://www.levelblue.com/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors>
22. AhnLab ASEC, Dire Wolf ransomware: threat combining data encryption and leak extortion (1 September 2025). <https://asec.ahnlab.com/en/89944/>
23. MyBroadband, Police emergency number 10111 offline for South African city with 5 million people (2 September 2026). <https://mybroadband.co.za/news/telecoms/665754-police-emergency-number-offline-for-south-african-city-with-5-million-people-as-10111-goes-down.html>
24. Furniture Bargaining Council, Preliminary cybersecurity notification, circular 11-26 (24 August 2026), rechecked 6 September 2026. <https://fbcweb.furnbed.co.za/>
25. MyBroadband, Largest parcel courier company in South Africa allegedly hit by cyberattack (18 August 2026). <https://mybroadband.co.za/news/security/662853-largest-parcel-courier-company-in-south-africa-allegedly-hit-by-cyberattack.html>
26. Babcock Africa, news index carrying the Babcock Africa update of 18 August 2026, rechecked 6 September 2026. <https://www.babcock.co.za/news/>
27. MyBroadband, Toyota South Africa sends warning about SMSs from its official line (12 August 2026). <https://mybroadband.co.za/news/security/662187-toyota-south-africa-sends-warning-about-smss-from-its-official-line.html>
28. Halcyon, Dire Wolf threat-actor profile (updated 13 November 2025). <https://www.halcyon.ai/threat-group/dire-wolf>
29. ransomware.live, per-group YARA, ransom-note and atomic indicator endpoints, retrieved 6 September 2026. <https://www.ransomware.live/>
30. ransomware.live, group index endpoint /groups, 396 groups, DireWolf recorded at 125 victims on 6 September 2026 against 115 on 30 August 2026. <https://www.ransomware.live/groups>
31. NVD CVSS base scores with scoring source, retrieved 6 September 2026. <https://nvd.nist.gov/>
32. Cybernews, CISA flags SonicWall SMA 1000 zero-day vulnerability, carrying the Shadowserver count (3 September 2026). <https://cybernews.com/security/cisa-flags-sonicwall-sma-1000-zero-day-vulnerability/>

33. BleepingComputer, CISA: SonicWall SMA1000 flaws now exploited by ransomware gangs (10 August 2026). <https://www.bleepingcomputer.com/news/security/cisa-sonicwall-sma1000-flaws-now-exploited-by-ransomware-gangs/>
34. BleepingComputer, SonicWall warns of actively exploited SMA1000 zero-day flaws (2 September 2026). <https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-actively-exploited-sma1000-zero-day-flaws/>
35. Rapid7, PaperCut NG/MF critical zero-day exploited in the wild (28 August 2026, updated 1 September 2026). <https://www.rapid7.com/blog/post/etr-papercut-ng-mf-critical-zero-day-exploited-in-the-wild/>
36. SecurityWeek, PaperCut exploitation escalates to active intrusions (1 September 2026). <https://www.securityweek.com/papercut-exploitation-escalates-to-active-intrusions/>
37. Kestra, GHSA-5vc5-wxxq-3fjx, unauthenticated RCE via authentication bypass in AuthenticationFilter (3 June 2026). <https://github.com/kestra-io/kestra/security/advisories/GHSA-5vc5-wxxq-3fjx>
38. Microsoft Security, When AI infrastructure becomes the target (26 August 2026). <https://www.microsoft.com/en-us/security/blog/2026/08/26/when-ai-infrastructure-becomes-target-securing-gateways-control-points/>
39. BleepingComputer, Hackers exploit critical JFrog Artifactory flaw to forge admin tokens (2 September 2026). <https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-jfrog-artifactory-flaw-to-forge-admin-tokens/>
40. GitHub Advisory Database, GHSA-86qp-5c8j-p5mr, Starlette missing Host header validation (21 May 2026). <https://github.com/advisories/GHSA-86qp-5c8j-p5mr>
41. BerriAI LiteLLM, GHSA-7488-6r32-c95q, MCP authentication bypass via OAuth2 passthrough fallback (30 June 2026). <https://github.com/BerriAI/litellm/security/advisories/GHSA-7488-6r32-c95q>
42. Wiz Threat Research, Inside 90 days of attacks on AI infrastructure (27 August 2026). <https://www.wiz.io/blog/ai-infrastructure-honeypot>
43. The Hacker News, LiteLLM flaw CVE-2026-42271 exploited in the wild, chains to unauthenticated RCE, quoting Horizon3.ai (9 June 2026). <https://thehackernews.com/2026/06/litellm-flaw-cve-2026-42271-exploited.html>
44. Sangoma, Switchvox release notes version 8.4.0.2, build 105309 (14 July 2026). <https://sangomakb.atlassian.net/wiki/spaces/Switchvox/pages/1802371073/Switchvox+-+Release+Notes+Version+8.4.0.2+July+14+2026>
45. Google, Chrome Releases: stable channel update for desktop (3 September 2026). https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html
46. FIRST, Exploit Prediction Scoring System scores, retrieved 6 September 2026. <https://www.first.org/epss/>
47. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 05:01 UTC 6 September 2026. <https://www.shodan.io/search?query=country%3AZA>
48. eSecurity Planet, Censys finds AI and LLM tool exposures up more than 60 per cent (23 July 2026). <https://www.esecurityplanet.com/threats/censys-finds-ai-llm-tool-exposures-up-more-than-60/>
49. SecurityWeek, 175,000 exposed Ollama hosts could enable LLM abuse (30 January 2026). <https://www.securityweek.com/175000-exposed-ollama-hosts-could-enable-llm-abuse/>
50. CyberDesserts, AI infrastructure scanning research (14 May 2026). <https://blog.cyberdesserts.com/ai-infrastructure-scanning-research/>
51. ITWeb, POPIA grace period limits regulator's fines (2 September 2026). <https://www.itweb.co.za/article/popia-grace-period-limits-regulators-fines/P3gQ2qGAIAk7nRD1>
52. Moonstone, New IT and cyber incident reporting template now in effect, reporting FSCA and Prudential Authority Joint Communication 5 of 2026 (3 September 2026). <https://www.moonstone.co.za/new-it-and-cyber-incident-reporting-template-now-in-effect/>
53. SARS, Scams and phishing index, most recent entry SARS-SCAM-399 (27 August 2026), checked 6 September 2026. <https://www.sars.gov.za/targeting-tax-crime/scams-and-phishing/>
54. BusinessTech, Warning about bank account takeovers in South Africa, reporting the SABRIC 2025 crime statistics released 4 August 2026 (1 September 2026). <https://businesstech.co.za/news/banking/872833/warning-about-bank-account-takeovers-in-south-africa/>
55. FIRST member teams. SA CSIRT records retrieved via the ransomware.live /csirt/ZA endpoint, 6 September 2026, six teams. <https://www.first.org/members/teams/>

TLP:CLEAR. 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.