



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 35 | 16 August – 22 August 2026

THREAT LEVEL: HIGH

TLP: CLEAR

Report ID: SA-CTI-2026-W35 | Classification: TLP: CLEAR

Published Monday 24 August 2026

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

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

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W35)
- 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, 18th consecutive week (16 August – 22 August 2026)

Story 1. MedusaLocker listed South Africa's largest express parcel courier on its leak site on 16 August 2026 and the company says it can find no sign of a breach.^{1,2} The Courier Guy told reporters the enquiry was the first it had heard of the claim, that it has no evidence of any internal system being compromised and is confident no customer data is involved. It has not notified the Information Regulator, on the stated basis that it has no information indicating a breach occurred, and says it will follow the POPIA process if the investigation finds otherwise.¹ The actor's post shows filenames rather than files and advertises the data for 30,000 US dollars, about R485,000. That price is the tell: MedusaLocker's recent posts routinely carry a fixed sum and the phrase "sale in one hand", which is a resale offer rather than a negotiated double-extortion demand.³ The rating is CLAIMED, because a leak-site description is written by the attacker and the denial is on the record; what settles it is what the investigation produces. First reported by [MyBroadband](#) on 18 August 2026.

Story 2. Nine vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 17 and 21 August, three times the previous week's three, and six were already past their remediation date on the day this report was published.⁴ Four map to products this report can count in South Africa, against one of three last week. The heaviest is Microsoft's Internet Key Exchange service extension, CVE-2026-33824, a double free reachable over UDP 500 and 4500 scored 9.8, patched by Microsoft in April 2026 and added to the catalogue on 18 August with a three-day deadline; neither agency has published any detail of the attacks.^{4,5,6} VMware vCenter CVE-2026-59310 is being exploited at scale, one responder counting 361 victim addresses across 47 countries by 7 August.^{7,8} Microsoft SharePoint CVE-2026-55040 forges an authentication token, has public exploit code, and 646 on-premises instances are exposed in South Africa.^{9,10,11}

Story 3. Three leak-site listings carried a South African country tag inside the window and one is not South African. Qilin listed Trends And Concepts on 20 August; the company is Trends and Concepts Total Interior Solutions of Makati in the Philippines, and a second tracker records what appears to be the same claim against trendsandconcepts.com.ph while describing the business correctly.^{2,12} A third aggregator repeated the South African tag and added a figure for people affected that the actor never published. The two that survive the check are The Courier Guy and Babcock, the South African arm of Babcock International Group, claimed by The Gentlemen on 19 August.^{2,13} Country and sector fields on these records are assigned by the aggregator rather than the victim, and this report treats them as leads. The week supplies the reason why.

Correction 1, to W34. Last week's edition named the Information Regulator's most recent publication as the enforcement notices of 2 June 2026 and put the interval at eleven weeks. Both are wrong. The Regulator issued a PAIA section 77J enforcement notice to the Gauteng Department of Health dated 8 June 2026, signed by the Chairperson and posted on 11 June.¹⁴ Measured from 8 June, the interval at last week's publication was ten weeks. It is eleven at this edition, so the printed figure is unchanged only because the previous one was a week out. The KPI table carries the corrected prior value and Section 8.1 sets out how the record was established.

1. 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>

2. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 122 records at filter purity 1.0, retrieved 05:00 UTC on 23 August 2026. <https://www.ransomware.live/>

3. ransomware.live, MedusaLocker group leak-site index, retrieved 23 August 2026. <https://www.ransomware.live/group/medusalocker>

4. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.21, released 21 August 2026, retrieved 23 August 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

5. NVD CVSS base scores with scoring source, retrieved 23 August 2026. <https://nvd.nist.gov/>

6. BleepingComputer, CISA: Critical Windows IKE extension flaw now exploited in attacks (19 August 2026). <https://www.bleepingcomputer.com/news/security/cisa-critical-windows-ike-extension-flaw-now-exploited-in-attacks/>

7. BleepingComputer, Critical VMware vCenter RCE flaw exploited for reverse SSH access (13 August 2026). <https://www.bleepingcomputer.com/news/security/critical-vmware-vcenter-rce-flaw-exploited-for-reverse-ssh-access/>

8. QUIRSO GmbH, Active exploitation of CVE-2026-59310: 361 victim IPs across 47 countries (August 2026). https://medium.com/@quirso_de/active-exploitation-of-cve-2026-59310-361-victim-ips-across-47-countries-9783187cc6ff

9. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 05:01 UTC on 23 August 2026. <https://www.shodan.io/search?query=country%3AZA>

10. The Hacker News, Attackers exploit SharePoint authentication bypass (13 August 2026). <https://thehackernews.com/2026/08/attackers-exploit-sharepoint.html>

11. Rapid7, Microsoft SharePoint JWT token authentication bypass, CVE-2026-55040 (11 August 2026). <https://www.rapid7.com/blog/post/ra-microsoft-sharepoint-jwt-token-authentication-bypass-cve-2026-55040/>

12. Breachsense, Trends and Concepts Total Interior Solutions data breach record, retrieved 23 August 2026. <https://www.breachsense.com/breaches/trends-and-concepts-total-interior-solutions-data-breach/>

13. Breachsense, Babcock International Group - Africa data breach record, discovered 20 August 2026, retrieved 23 August 2026. <https://www.breachsense.com/breaches/babcock-international-group-africa-data-breach/>

14. Information Regulator of South Africa, Gauteng Department of Health enforcement notice, PAIA section 77J Form H, dated 8 June 2026. <https://inforegulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>

KPI Dashboard

Metric	Current (W35)	Prior (W34)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (18th week)	FLAT
ransomware.live SA cumulative	122	119	+3	UP
SA claims dated inside the window	3	0	+3	UP
Window claims surviving the nationality check	2 of 3	n/a (metric added W35)	n/a	n/a
SA breaches confirmed by the victim	0	3	-3	DOWN
New CISA KEV additions	9	3	+6	UP
KEV adds already overdue at publication	6	2	+4	UP
KEV adds with a VERIFIED SA exposure figure	4 of 9	1 of 3	+3	UP
Corrections issued to prior editions	1	3	-2	DOWN
Weeks since last IR publication	11	10 (corrected)	+1	UP

W35 KEY FRAMING: last week every South African incident was confirmed by the organisation it happened to. This week none was. Two companies were named by ransomware groups and neither has acknowledged a compromise, which leaves the domestic picture resting on what attackers say about their victims. Actor claims are the weakest evidence this report handles, and one of the three South African listings turned out to describe a company in Makati. The solid material sits on the vulnerability side: nine catalogue additions in five days, among them a pre-authentication remote code execution flaw in a Windows service switched on wherever IPsec is used, a vCenter flaw with 361 counted victims, and a SharePoint token forgery with public exploit code and 646 exposed South African instances. The board question is narrow and answerable: of those nine products, which do you run, and how long did it take to find out. An organisation that can answer in an afternoon has an asset inventory. One that cannot has six overdue jobs it has not yet identified.

TOP 3 ACTIONS THIS WEEK

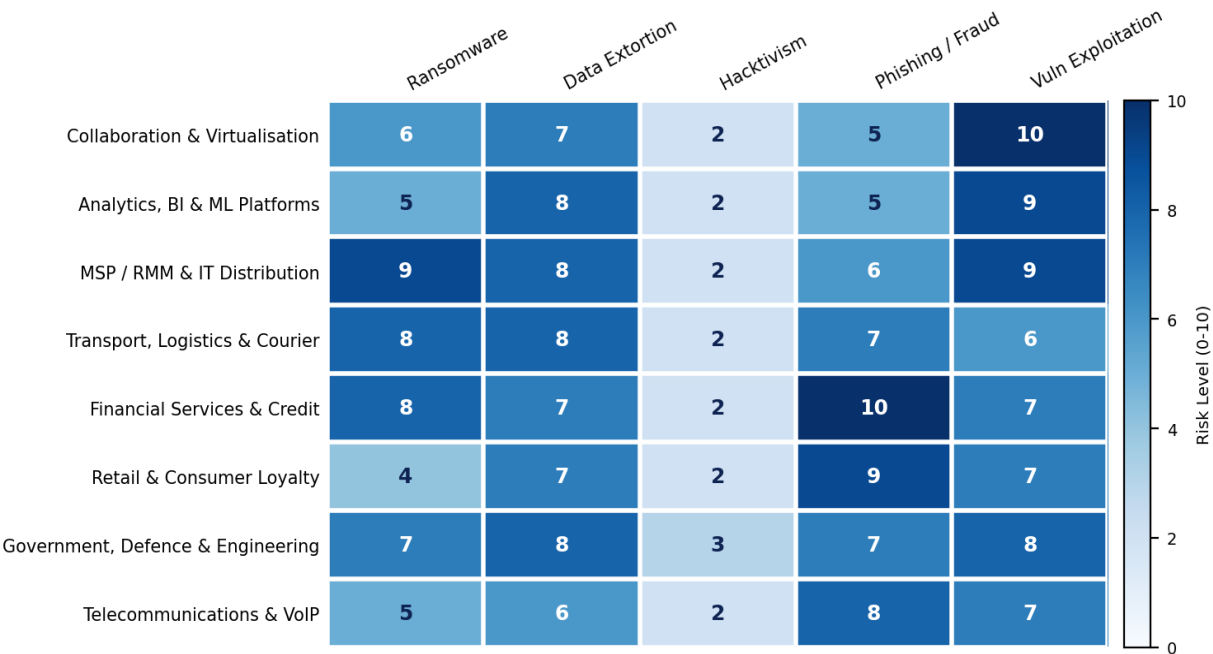
1. Work the nine catalogue additions against a real inventory on Monday 24 August, starting with the six already overdue. In deadline order: Ray below 2.52.0 was due 20 August; Windows IKE, VMware vCenter, on-premises SharePoint and macOS were due 21 August; TrueConf Server was due 23 August; Zimbra is due on 24 August itself. Fixed versions are in the Section 5 table. Where you cannot patch immediately, block inbound UDP 500 and 4500 on any Windows host that does not terminate IPsec, block TCP 4307 to TrueConf servers, remove the zimbra-snmp package or disable SNMP notifications, and take the Ray dashboard on 8265 off any interface a browser can reach.

2. Patch on-premises SharePoint and hunt for forged tokens. CVE-2026-55040 lets an attacker mint a JSON web token that SharePoint accepts as any user, including a site administrator, and it is fixed in the July 2026 update. Rapid7 published the technical chain on 11 August and a working proof of concept went with it; Defused Cyber reported exploitation using that code within two days, and attempts against the flaw date back to 19 July. There are 646 on-premises SharePoint instances exposed in South Africa, which is an exposure count and not a count of vulnerable systems, but it is the population an untargeted scanner sees. Hunt for tokens whose outer header carries alg set to none and an x5t thumbprint matching the server's own security token service certificate.

3. If a ransomware group names your organisation, run an evidence-led investigation before you run a denial. The Courier Guy's opening position is reasonable, and it is a position rather than a finding. The work that converts one into the other is bounded: reconcile the actor's claim of extracted emails against mail export and search-audit logs, check remote desktop and VPN authentication for the fortnight before 16 August because exposed remote desktop is this group's documented primary entry route, and confirm whether the filenames on the leak post correspond to real documents. Then form a POPIA section 22 view in writing, because the trigger is a reasonable belief that personal information was accessed by an unauthorised person rather than certainty.

2. THREAT LANDSCAPE HEATMAP

South African Sector Threat Levels, Week 35 (16 - 22 August 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 is scored on its standing exposure.

Three rows changed value and two were renamed. **Collaboration and Virtualisation Platforms enters at 10 for vulnerability exploitation**, the highest cell in the matrix, because four of the nine catalogue additions sit in it: SharePoint, vCenter, Zimbra and TrueConf. A new row enters at a value rather than rising to one. **Transport, Logistics and Courier enters at 8** for ransomware and data extortion on the MedusaLocker claim, and at 7 for phishing and fraud on ESET's reporting of South African delivery scams timed to genuine orders. **Analytics and Business Intelligence is renamed Analytics, BI and ML Platforms** because MLflow and Ray both entered the catalogue and both now carry South African exposure figures; the rename reflects scope and the row keeps its 9, since Metabase already held it there. **Government and State-Owned Enterprises widens to Government, Defence and Engineering** and rises to 7 for ransomware on the Babcock listing. **Financial Services and Credit holds 10 for phishing and fraud**, the only other maximum cell, on the Absa disclosure of a R129 million increase in fraud-driven operational losses and on vendor reporting of banking trojans impersonating four South African brands. Automotive and Dealer Networks and Professional and Business Services retire: the Toyota investigation produced nothing new and neither sector had an observation to score.

3. TOP SA INCIDENTS (W35)

Two ransomware groups named South African organisations in the window and neither has acknowledged a compromise, so both sit at CLAIMED. The only item carrying a victim's own signature is a financial disclosure rather than a breach. The three are set out weakest evidence first.

3.1 INC-2026-W35-01: The Courier Guy, MedusaLocker Leak-Site Claim and Company Denial [CLAIMED]

Sector	Transport, logistics and courier
Named organisation	The Courier Guy, thecourierguy.co.za, South Africa's largest express parcel and e-commerce courier
Actor and listing	MedusaLocker, a ransomware-as-a-service operation active since at least 2019. Listed 16 August 2026, 15:19 UTC, estimated attack date the same day
Actor claim	Emails extracted; leak post shows filenames only, with a stated sale price of 30,000 US dollars, about R485,000
Company position	First heard of the claim through a press enquiry. No evidence of any internal system compromised. Confident no customer data is involved. Regulator not notified, on the stated basis that it has no information indicating a breach occurred, with the POPIA process to follow if the investigation finds otherwise
Confidence	CLAIMED. Threat-actor assertion, no independent corroboration, and an on-the-record denial by the named organisation

The victim feed recorded a MedusaLocker listing for The Courier Guy on 16 August 2026, with the description "Organization with 2018 emails extracted" against the domain thecourierguy.co.za; the country and sector fields are the aggregator's own.² Approached for comment, the company said the enquiry was the first it had heard of any alleged attack and that MedusaLocker had not contacted it. Its two substantive statements are both qualified, and the qualifications matter in a live investigation: it has "no evidence at this stage of any internal systems being compromised", and "from what we've been able to review of the material referenced" it is confident no customer data is involved, the second describing a review of the leak-site material rather than of its own systems. It said it has not notified the Information Regulator because it currently has no information indicating a breach occurred, and that it would follow the appropriate POPIA notification process if the investigation found otherwise.¹ First reported by [MyBroadband](#) on 18 August 2026.

Two features of the post are worth separating from whether it is true. The stated price is the first: some MedusaLocker listings advertise a fixed sum with the phrase "sale in one hand", at prices running from roughly 20,000 to 160,000 US dollars, which is an offer to sell a dataset once to a single buyer rather than a countdown against a victim expected to negotiate, and that changes what a response looks like.³ The second is that filenames rather than files are shown, which is consistent with a real extraction held back as proof and equally consistent with a listing built on material that does not support the claim. Neither reading can be preferred from outside and what settles it is inside the company. The tests are whether mail

export and search-audit logs show a bulk extraction in the fortnight to 16 August, and whether remote desktop and VPN records show access nobody can account for, remote desktop being this group's documented primary entry route.¹⁵ A denial rests on that behaviour not being found, which requires looking for it. **Detection relevance:** TH-2026-W35-01 carries the hunt with sourced sample hashes and the group's YARA rule.

1. 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>

2. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 122 records at filter purity 1.0, retrieved 05:00 UTC on 23 August 2026. <https://www.ransomware.live/>

15. FBI, CISA, Department of the Treasury and FinCEN, #StopRansomware: MedusaLocker, product AA22-181A (30 June 2022), retrieved from the FBI IC3 mirror because cisa.gov returns an empty body to this environment. <https://www.ic3.gov/CSA/2022/220630.pdf>

16. Kaspersky Securelist, The Gentlemen RaaS: rapid growth and a new ransomware variant (29 June 2026). <https://securelist.com/the-gentlemen-raas/120447/>

3.2 INC-2026-W35-02: Babcock South Africa, The Gentlemen Leak-Site Claim [CLAIMED]

Sector	Engineering, asset management and defence support
Named organisation	Babcock, domain babcock.co.za, the South African arm of Babcock International Group
Actor and listing	The Gentlemen, tracked by Microsoft as Storm-2697, active since at least July 2025. Listed 19 August 2026, 08:10 UTC, tagged Government and Defence by the aggregator
Actor claim	Company profile text only. No dataset, sample, file tree or claimed record count published at the time of writing
Corroboration and response	A second independent tracker records the same claim against the same domain, discovered 20 August 2026. No statement located from either the South African business or the parent group
Confidence	CLAIMED. Two trackers observing the same actor post is not two sources for the underlying compromise

The Gentlemen listed Babcock against the domain babcock.co.za, recorded by the victim feed on 19 August 2026 and by a second tracker on 20 August under the name Babcock International Group Africa, with the leak size unknown.^{2,13} No dataset, sample or claimed record count accompanies it. The aggregator record carries a description of the business as an engineering and asset management company in critical infrastructure and heavy equipment across the African continent, which points at the South African operation rather than the United Kingdom parent; that text is the tracker's own enrichment rather than the actor's post, since the field begins with the domain and a RocketReach profile URL, so it is weak evidence of what the actor actually claimed.² Two trackers indexing the same leak-site post is one observation seen twice, and the rating stays at CLAIMED until Babcock says something or a dataset appears.

The entity question is worth resolving now rather than after someone repeats it wrongly. The claim is against the South African domain and the group's own description is of the African business; nothing located supports a claim against Babcock International Group in the United Kingdom. Both trackers publish credential-exposure telemetry for the domain alongside the claim, and one cautions that the telemetry is not necessarily connected to it.¹³ That caution is correct and this report repeats it: harvested credentials for a domain are a standing condition of doing business on the internet and are not evidence

that a particular intrusion happened.

What raises this above a routine listing is the actor, profiled in Section 4.2. Its documented initial access is exploitation of internet-facing firewalls and VPNs, brute force, purchased or leaked credentials and access brokers, and its deployment spreads the encryptor to every domain-joined computer through Group Policy from a domain controller, with self-propagation over SMB and the NETLOGON share.^{16,17} An organisation named by this group that finds nothing should still check Group Policy objects and the NETLOGON share, because the deployment mechanism leaves traces where an endpoint-only investigation will not look. **Detection relevance:** TH-2026-W35-02.

2. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 122 records at filter purity 1.0, retrieved 05:00 UTC on 23 August 2026. <https://www.ransomware.live/>

11. Rapid7, Microsoft SharePoint JWT token authentication bypass, CVE-2026-55040 (11 August 2026). <https://www.rapid7.com/blog/post/ra-microsoft-sharepoint-jwt-token-authentication-bypass-cve-2026-55040/>

3.3 INC-2026-W35-03: Absa, R129 Million Increase in Fraud-Driven Operational Losses [CONFIRMED]

Sector	Financial services and credit
Organisation and disclosure	Absa Group, interim results for the six months to 30 June 2026
Figure	Operational risk losses rose by R129 million to R369 million, from R240 million in the comparable period
Attribution by the bank	Largely increased digital fraud driven by increasingly sophisticated social engineering and malicious applications targeting customer devices
Context	Other operating costs including net fraud losses grew 41 per cent. Profit attributable to ordinary equity holders rose 12 per cent to R12.6 billion; headline earnings, the bank's own headline measure, rose 8 per cent to R12.8 billion. Total IT spend rose 7 per cent to R8.8 billion, 28 per cent of group expenses
Confidence	CONFIRMED as a disclosure by the organisation. The operational risk loss figures are quoted from the results by national technology press; they sit in the risk-management section of the results booklet, which this report could not retrieve directly, so they are confirmed via reporting rather than read at the primary

Absa's interim results record operational risk losses of R369 million for the six months to 30 June 2026, R129 million higher than the R240 million of the comparable period, and the bank attributes the increase largely to digital fraud driven by social engineering and malicious applications on customer devices.¹⁸ This is the only item in the section with a number the affected organisation stands behind, and it belongs in a threat report for a reason that has nothing to do with Absa. It prices the thing that most South African organisations describe qualitatively. A bank with R8.8 billion of technology spend, in-application malware detection, call screening and real-time customer alerting still absorbed a R129 million increase, which is a statement about where the attack has moved rather than about that bank's controls. First reported by [MyBroadband](#) on 20 August 2026.

Separately from the results, Absa's Daniel Munslow has said the bank has not observed any abnormal increase in card skimming during 2026, attributing the decline largely to chip and PIN adoption and

improved fraud prevention, a view Capitec echoed; the reported growth is in phishing and voice-phishing-assisted account takeover, and in card swapping.¹⁸ Two vendor observations in the same window point the same way. NordVPN describes a campaign distributing Android applications that impersonate Takealot, DStv, South African Airways and SARS. Each requests SMS, contacts, call log, screen capture, audio and camera permissions together, and the capability that matters is interception of the SMS one-time password, which defeats the second factor on a banking login. NordVPN counts more than a hundred campaign domains, registered on disposable extensions such as .cc, .lol, .xyz and .mom and almost all fronted by Cloudflare. The campaign is global and these four brands are its South African localisation; Kaspersky is quoted in the same report on South African credential targeting generally rather than on this campaign.¹⁹ ESET's Allan Juma describes South African courier scams that mirror real delivery workflows closely. The finding that virtual cards do not protect the victim, because the rotating security code is validated only once when the card is tokenised into a digital wallet, is the publication's own reporting rather than ESET's.²⁰ Both rest on vendor telemetry with no named victim, so both are PROBABLE. **Detection relevance:** no hunt mission is issued, because neither researcher published atomic indicators and this report does not invent them; the controls are in Section 10.

12. Breachsense, Trends and Concepts Total Interior Solutions data breach record, retrieved 23 August 2026.

<https://www.breachsense.com/breaches/trends-and-concepts-total-interior-solutions-data-breach/>

46. N-able, N-central security update, 10 August 2026 (modified 13 August 2026).

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

48. FIRST, member teams directory. South African CSIRT records retrieved through the ransomware.live /csirt/ZA endpoint on 23 August 2026, six teams. <https://www.first.org/members/teams/>

3.4 Carryovers

LEGO Certified Stores South Africa, Marsello and Metabase, W34. A second South African publication carried the story on 17 August, but it credits and links the original reporting and adds no independent account, so the incident remains single-sourced.²¹ It records that Marsello has confirmed no further unauthorised access since the patch, and that further unauthorised access is considered highly unlikely, which in the underlying notice is the retailer's opinion rather than Marsello's, and that LEGO Certified Stores is reviewing security and access controls with its service providers. No standalone Marsello statement has been located and no second South African brand on the same platform has notified. Status unchanged at CONFIRMED. South African Metabase instances counted 109 at this collection, against an actively exploited flaw with public exploit code.⁹

Toyota South Africa Motors, W34. No development in the window. The company has declined to name the third-party bulk SMS provider while the matter is under investigation and referred to the authorities, so no other South African organisation can determine whether it shares that supplier.²² The company's site is client-side rendered and could not be read here, so a primary notice may exist unverified. Status unchanged at CONFIRMED with an unnamed supplier.

Euphoria Telecom and Fidelity Services Group. No development in the window for either. Statuses unchanged.

DC Partner, Buzz Trading 104 and Serengeti Estates, W33. All three remain CLAIMED. No dataset has surfaced, no further Krybit listing has appeared against South Africa across the two subsequent windows, and the National Credit Regulator has not commented publicly on DC Partner.²

15. FBI, CISA, Department of the Treasury and FinCEN, #StopRansomware: MedusaLocker, product AA22-181A (30 June 2022), retrieved from the FBI IC3 mirror because cisa.gov returns an empty body to this environment. <https://www.ic3.gov/CSA/2022/220630.pdf>
16. Kaspersky Securelist, The Gentlemen RaaS: rapid growth and a new ransomware variant (29 June 2026). <https://securelist.com/the-gentlemen-raas/120447/>
17. Palo Alto Networks Unit 42, No manners here: the ruthless rise of The Gentlemen ransomware (10 July 2026). <https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/>
18. MyBroadband, Major bank in South Africa takes R129-million cyber fraud hit (20 August 2026). <https://mybroadband.co.za/news/security/663249-major-bank-in-south-africa-takes-r129-million-cyber-fraud-hit.html>
19. MyBroadband, DStv, Takealot and South African Airways impersonated to take over bank accounts in South Africa (20 August 2026), reporting NordVPN and Kaspersky research. <https://mybroadband.co.za/news/security/663273-dstv-takealot-and-south-african-airways-impersonated-to-take-over-bank-accounts-in-south-africa.html>
20. MyBroadband, Criminals targeting people who shop online in South Africa (19 August 2026), reporting ESET analysis. <https://mybroadband.co.za/news/security/661906-criminals-targeting-people-who-shop-online-in-south-africa.html>
21. The Citizen, Zero-day hack exposes Lego Certified Stores SA customer data (17 August 2026). <https://www.citizen.co.za/lifestyle/technology/zero-day-hack-exposes-lego-certified-stores-sa-customer-data/>
22. 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 groups named South African organisations this week and they stand in different relationships to the country. MedusaLocker has never listed a South African victim before. The Gentlemen has listed six since January and Babcock is its seventh, which makes this a resumption rather than an arrival. A third group is profiled because it produced the week's mis-attributed listing. Head Mare, whose campaign put both TrueConf flaws into the catalogue, is covered in Section 5 and TH-2026-W35-05 rather than profiled here, since it has no observed South African activity. Fourteen groups have been active against South Africa in the last 120 days on the aggregator's reckoning: Black X, PrinzEugen, arcusmedia, cmdorganization, dragonforce, incransom, krybit, m3rx, medusalocker, payload, qilin, ransomhouse, stormous and thegentlemen. The list grew by two, medusalocker and qilin, the latter entering on the listing this report rules non-South-African in Section 4.3, which is a caution about the group-count metric as much as about the listing.

4.1 MedusaLocker: An Old Operation With a Resale Business Model

MedusaLocker has run as a ransomware-as-a-service operation for years and was the subject of a joint FBI, CISA, Treasury and FinCEN advisory, product AA22-181A, published on 30 June 2022, for which no revision has since been published.¹⁵ The advisory's own framing is activity observed as recently as May 2022; the 2019 origin date commonly attached to this group is not in it. That advisory remains the best description of its tradecraft: primary access through vulnerable remote desktop configuration, with phishing and spam campaigns attaching the payload directly as the secondary route; propagation by a PowerShell reflective injection script that edits the EnableLinkedConnections registry value and restarts the LanmanWorkstation service; security, accounting and forensic processes killed and the host rebooted into safe mode before encryption; AES-256 file encryption with an RSA-2048 wrapped key on a sixty-second loop; persistence as svhost.exe or svhostt.exe in the roaming application data directory with a scheduled task every fifteen minutes. Affiliates take 55 to 60 per cent of paid ransoms.¹⁵ The detection detail is in TH-2026-W35-01.

Two things about the South African listing sit outside that description. The advisory says the size of demands appears to vary with the victim's perceived financial status, which reads as a negotiation-led rather than a fixed-tariff model, though the advisory does not use those words. Against that, some of the group's leak-site posts advertise a dataset at a stated fixed price with the phrase "sale in one hand": 120,000 US dollars for a United States energy firm listed in September 2025 and 40,000 for a Canadian technology firm in November 2025, with stated prices across its listings running from roughly 20,000 to 160,000. The Courier Guy post at 30,000 sits inside that range.^{1,3} The phrase appears on a minority of posts rather than on all of them, and no vendor or government analysis characterising a shift in monetisation has been located, so this is recorded as a leak-site observation rather than as attribution of a strategy. Second, a resale posting does not require encryption to have happened, which is consistent with a company reporting no operational disruption while a claim exists. The relevant South African exposure figure is remote desktop: 7,767 services counted on port 3389, an exposure count rather than a count of vulnerable systems, and the population this group's documented primary access route addresses.⁹ One disambiguation prevents a common error: Medusa, whose advisory the FBI, CISA and HHS updated on 18 August, is a different operation, and the FBI says so in the advisory itself.^{23,24}

4.2 The Gentlemen, Storm-2697: Scale, and a Group Policy Problem

Microsoft tracks the operators behind The Gentlemen as Storm-2697, a financially motivated actor running the platform while affiliates carry out the attacks.²⁵ Unit 42 records the programme as active since at least July 2025, operators likely active earlier as a Qilin affiliate, variants in both C and Go, and an unusual 90 per cent affiliate payout against a typical 70 to 80.¹⁷ The volume figures are snapshots at different dates rather than competing claims: 580 victims across 77 countries to 7 July 2026, of which 103 were manufacturers, and 778 in the group feed retrieved with this edition's collection run.^{17,26} Cyble's research, as rendered by its own publication, puts the group at 56 attacks in the Middle East and Africa in the first half of 2026, more than a quarter of regional ransomware incidents; that is the two regions together and for six months, and should not be compressed into an African figure. That figure comes from a Cyble report held behind a registration form and could not be checked at the primary, so it is withdrawn from this edition and replaced by Cyble's Annual Threat Landscape Report 2025, which was obtained directly. That report puts The Gentlemen at 63 victims in 2025 and ranks it among the most prolific of the fifty-seven ransomware groups that emerged that year, behind Sinobi at 138, NightSpire at 92 and Warlock at 66.²⁷ For regional context it counts 202 ransomware victims across its combined Middle East, Turkiye and Africa region for the whole of 2025, with Turkiye at 29, the United Arab Emirates at 27 and Saudi Arabia at 22 as the most affected countries; South Africa does not appear in that top three.²⁷ Other African victims on the aggregator's recent listings are Bouri Group in Egypt in June and SETCAR in Tunisia in May, which is not a complete list because that view shows recent entries only. South Africa is not new ground for this group: the victim feed holds six South African listings between 20 January and 19 April 2026, being Paltrack, Rola Motor Group and Witzenberg Municipality on one day in January, Intsika Yethu Municipality in February, Elundini in March and Sunspray Food in April.² Babcock is the seventh and the first in four months, so the framing that fits is a resumption after a pause rather than a new interest in the country.²⁶

The operational detail to act on is the deployment mechanism. Kaspersky documents a command-line flag on the encryptor, designed to run on a domain controller, that spreads the payload to every domain-joined computer through Group Policy by writing and executing `deploy_gpo.ps1` in the temporary directory, and separately uses the NETLOGON share to distribute the executable. The same research documents bring-your-own-vulnerable-driver defence evasion using seven named signed drivers, plus Windows

Kernel Explorer and OpenArk64 to remove security drivers.¹⁶ Microsoft adds that the Go encryptor attempts, across all its techniques, twenty-one remote execution operations per target host, clears the System, Application and Security logs with wevtutil, and deletes shadow copies with both vssadmin and wmic.²⁵ An organisation named by this group that finds nothing on endpoints has not finished looking. The hunt is TH-2026-W35-02.

4.3 Qilin, and What a Country Tag Is Worth

Qilin operated first as Agenda before taking the Qilin name; Trend Micro documented the migration of its payload from Go to Rust in December 2022, describing Agenda and Qilin as the same operation.²⁸ The precise rebrand month and the language of the Linux and ESXi locker are not established by that source and are not asserted here. On volume, Cyble's Annual Threat Landscape Report 2025 records Qilin as the most active ransomware group of 2025 in every region it measures: 634 victims in the Americas, 204 in Europe and the United Kingdom, 105 in Asia and Oceania, and 21 in the combined Middle East, Türkiye and Africa region.²⁷ The aggregator's all-time tally agrees, putting Qilin first among all tracked groups at 2,195 victims against The Gentlemen's 778, while Unit 42 records The Gentlemen as the second most active programme of 2026 specifically.^{17,26} Qilin's lead is cumulative and the 2026 quarterly rankings have moved between the two. Its South African relevance this week is negative and instructive: the Trends And Concepts listing of 20 August is tagged South African on the aggregator this report uses, and the company is an interior fit-out firm headquartered in Makati in the Philippines. A second tracker records what appears to be the same claim, against the domain trendsandconcepts.com.ph, and describes the business correctly; the two record different domains for it and differ by a day on the discovery date, so the match is an inference rather than a certainty. A third aggregator repeated the South African tag and attached a figure for people affected that does not appear in the actor's post.^{2,12}

This is the second consecutive month in which an aggregator country field has misplaced a victim into South Africa; W33 recorded two Costa Rican companies tagged South African and a sector field that contradicted the actor's own text. The standing rule matters here: country and sector fields on these records are assigned by the aggregator rather than the victim, and they are leads rather than facts. The check costs a few minutes, being a look at the claimed domain, its registration and the company's own site, and this week it removed a third of the apparent South African listing volume. The KPI table carries the result as a row from this edition.

23. FBI, CISA and HHS, #StopRansomware: Medusa ransomware, product AA25-071A, originally published 12 March 2025, last updated 18 August 2026, retrieved from the FBI IC3 mirror. <https://www.ic3.gov/CSA/2026/260818.pdf>

24. American Hospital Association, Agencies issue update on Medusa ransomware activity (19 August 2026). <https://www.aha.org/news/headline/2026-08-19-agencies-issue-update-medusa-ransomware-activity>

25. Microsoft Threat Intelligence, The Gentlemen ransomware: dissecting a self-propagating Go encryptor (28 May 2026). <https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/>

26. ransomware.live, group statistics and per-group victim records, 778 victims recorded for The Gentlemen, retrieved with the 05:00 UTC collection run of 23 August 2026. <https://www.ransomware.live/groupstats/thegentlemen>

27. Cyble, Annual Threat Landscape Report 2025 (copyright 2026 Cyble Inc.), obtained by completing the publisher's registration. Not linkable without registration.

28. Trend Micro, Agenda ransomware uses Rust to target more vital industries (16 December 2022). https://www.trendmicro.com/en_us/research/22/1/agenda-ransomware-uses-rust-to-target-more-vital-industries.html

5. CRITICAL VULNERABILITIES & CISA KEV

Nine vulnerabilities entered the CISA catalogue of known exploited vulnerabilities between 17 and 21 August 2026, against three the week before, in catalogue version 2026.08.21.⁴ Six were past their remediation date when this report was published on Monday 24 August: Ray by four days, the four 18 August additions by three days each, and one of the two TrueConf entries by one day. Zimbra is due on 24 August itself. Due dates are per entry rather than a uniform interval and the required action cites CISA Binding Operational Directive 26-04.⁴ All nine carry a knownRansomwareCampaignUse value of Unknown, which the catalogue distinguishes from no. All CVSS values below are NVD base scores; where a score is CVSS 4.0 it is labelled, because 4.0 and 3.1 figures are not directly comparable.⁵

Microsoft Internet Key Exchange service extensions, CVE-2026-33824 is the one to read first: a double free in the IKEv2 fragment reassembly path scored 9.8, reachable by crafted UDP packets to ports 500 and 4500, giving code execution as the IKEEXT service and therefore as SYSTEM, across supported Windows 10, Windows 11 and Windows Server builds with IKEv2 enabled. Microsoft addressed it in the April 2026 security update, four months before CISA listed it as exploited, so the population at risk is defined by patch lag rather than patch availability.^{6,29} Neither CISA nor Microsoft has published any detail of the observed attacks: a CISA spokesperson said the agency had nothing further to share, and Microsoft's statement went no further than recommending the April update. This report has seen an unsourced claim attributing the activity to a named actor and does not repeat it.⁶ Where patching lags, block inbound UDP 500 and 4500 on hosts that do not terminate IPsec or restrict them to known peers. Its EPSS score of 0.7790 is the highest of the nine.³⁰

Broadcom VMware vCenter, CVE-2026-59310 is the one with counted victims: a directory traversal in the vCenter Syslog server scored 9.8, disclosed by Broadcom on 29 July with no workaround beyond patching. The German incident response firm QUIRSO, working a live engagement, recorded 361 unique victim addresses across 47 countries by 7 August, with the open-source reverse_ssh framework installed through a cron job for persistence and command and control.^{7,8} Its position has since moved. In a second publication on 15 August QUIRSO assessed with moderate confidence that the campaign is run by a Chinese-speaking actor probably working in a UTC+8 environment, on the convergence of Chinese-language artefacts in attacker scripts, apparent reuse of research from a Chinese security publication, Chinese-language tooling, and victimology that excludes mainland China. It published its indicators rather than continuing to withhold them, reported co-exploitation of CVE-2026-59309, and documented Babuk-derived ransomware carrying a .babyk extension deployed to ESXi hosts, which encrypted the ESXi logs and destroyed the telemetry an investigation would otherwise have used.³¹ QUIRSO cautions that the Babuk-derived payload is weak attribution evidence in itself, the builder having leaked in 2021, and that the choice may be opportunistic or deliberately misdirecting.³¹ Four instances are exposed in South Africa, a small number that understates the risk, because vCenter is normally internal and therefore reachable from anywhere an attacker already has a foothold.⁹

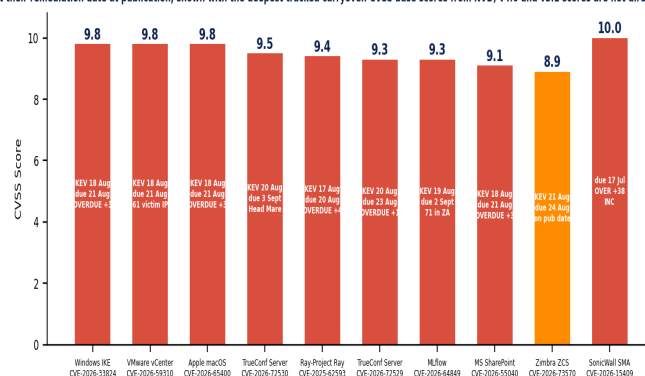
Microsoft SharePoint, CVE-2026-55040 has the largest South African footprint: a weak authentication flaw scored 9.1, fixed in the July 2026 update, affecting SharePoint Enterprise Server 2016, SharePoint Server 2019 and Subscription Edition. Rapid7 published the chain on 11 August and it runs to four weaknesses: an outer token header declaring no algorithm; an actor token whose x5t header carries SharePoint's own security token service certificate thumbprint, so the signing key resolves without

verification; that certificate not being present in TrustedSecurityTokenServices, so the issuer is accepted anyway; and an inner signature that is non-empty and never checked. The result is a forged token that impersonates any site user or administrator.^{10,11} A Python proof of concept shipped with it, and Defused Cyber reported exploitation using that code within two days, with KEVINtel telemetry recording eight of twelve tracked attempts on 12 and 13 August. Attempts against the flaw date back to 19 July, so the proof of concept produced a spike rather than the first activity.¹⁰ There are 646 on-premises instances exposed in South Africa.⁹

The remaining six. Zimbra Collaboration Suite CVE-2026-73570, 8.9, is an OS command injection in SNMP notification processing, reached by specially crafted SMTP requests, that applies only where the optional zimbra-smnp package is installed and SNMP notifications are enabled, fixed in 10.1.20, with CERT Polska confirming exploitation.³² Blocking SNMP alone does not close it, because SMTP is the delivery channel and the notification handler is the vulnerable code. TrueConf Server CVE-2026-72530 and CVE-2026-72529 are the sandbox escape and the missing authentication that Head Mare chains over TCP 4307, fixed in 5.3.9, 5.4.9 and 5.5.5.^{33,34} Their scores need care: NVD gives 9.5 and 9.3 under CVSS 4.0 while the vendor publishes 9.0 and 9.8 under CVSS 3.1, which reverses which of the pair looks worse. The vendor ordering matches operational reality, since the missing authentication is the unauthenticated entry point on 4307 and the sandbox escape is the follow-on. MLflow CVE-2026-64849, 9.3, is an unauthenticated server-side request forgery in the model registry webhooks API that follows redirects without revalidating the destination, so a redirect to a cloud metadata address returns the response body to the attacker, with DNS rebinding as a second path past the same guard; fixed in 3.15.0. watchTower reported indiscriminate scanning for exposed instances within hours of the identifier being assigned on 17 August, and credential theft from cloud-hosted instances thereafter.^{35,36} Apple macOS CVE-2026-65400, 9.8, allows network authentication to Screen Sharing without valid credentials, fixed 6 August in Tahoe 26.6.1, Sequoia 15.7.9 and Sonoma 14.8.9, and is being used on Macs with port 5900 exposed to obtain root and install a Monero miner.^{37,38,39} Ray CVE-2025-62593, 9.4, is a code injection in the unauthenticated Ray dashboard API on port 8265 whose browser check trusted a User-Agent beginning Mozilla, which the fetch implementations in Firefox and Safari let a page override. Exploitation requires a DNS rebinding attack against a developer's browser rather than direct access to the server, so the exposure count below is the population at risk only where a developer can be lured to a malicious page. Fixed in 2.52.0.^{40,41}

W35 CVSS Severity Distribution

W35 KEV / CRITICAL CVE SEVERITY | 16 - 22 August 2026
Nine KEV additions in the window, six already past their remediation date at publication, shown with the deepest tracked carryover. CVSS base scores from NVD; v4.0 and v3.1 scores are not directly comparable and the version is given per entry in the table



W35 CISA KEV / Critical CVE Tracking (nine additions 17 to 21 August plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-33824	Microsoft IKE Service Extensions	9.8	Double free (unauth RCE)	21 Aug	KEV 18 Aug. OVERDUE +3. UDP 500 and 4500, code execution as SYSTEM. Patched April 2026. No exploitation detail published. No Shodan label, so no ZA figure. Ransomware: Unknown. EPSS 0.7790, highest of the nine.
CVE-2026-59310	Broadcom VMware vCenter	9.8	Path traversal (unauth RCE)	21 Aug	KEV 18 Aug. OVERDUE +3. 361 victim IPs, 47 countries, by 7 Aug; reverse_ssh via cron. No workaround. Fixed 9.1.0.0300 / 9.0.2.0100 / 8.0 U3k / 8.0 U2f. 4 in ZA. Ransomware: Unknown.
CVE-2026-65400	Apple macOS	9.8	Improper authentication	21 Aug	KEV 18 Aug. OVERDUE +3. Screen Sharing bypass on TCP 5900; root plus XMRig observed. Fixed Tahoe 26.6.1 / Sequoia 15.7.9 / Sonoma 14.8.9, all 6 Aug. Shodan zero in ZA, held not published.
CVE-2026-72530	TrueConf Server	9.5	Code injection (sandbox escape)	3 Sept	KEV 20 Aug. Ten days to run. Chained after CVE-2026-72529 over TCP 4307. Head Mare, PhantomCore. Fixed 5.3.9 / 5.4.9 / 5.5.5. No Shodan label. EPSS 0.0097.
CVE-2025-62593	Ray-Project Ray	9.4	Code injection (unauth RCE)	20 Aug	KEV 17 Aug. OVERDUE +4. Dashboard API on 8265; browser check bypassed via Firefox and Safari User-Agent override. Fixed 2.52.0. 54 in ZA. EPSS 0.0100.
CVE-2026-72529	TrueConf Server	9.3	Missing authentication	23 Aug	KEV 20 Aug. OVERDUE +1. Unauthenticated script execution via TCP 4307, open by default. Fixed 5.3.9 / 5.4.9 / 5.5.5. EPSS 0.0079.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-64849	MLflow	9.3	SSRF (unauth)	2 Sept	KEV 19 Aug. Nine days to run. Webhooks test endpoint follows redirects without revalidation, reaching cloud metadata. Fixed 3.15.0. 71 in ZA. EPSS 0.0815.
CVE-2026-55040	Microsoft SharePoint	9.1	Weak authentication (JWT forgery)	21 Aug	KEV 18 Aug. OVERDUE +3. Fixed in the July 2026 update. Public PoC 11 Aug; Defused Cyber reported exploitation with it 12 to 13 Aug, though attempts date to 19 Jul. 646 in ZA. EPSS 0.0549.
CVE-2026-73570	Synacor Zimbra Collaboration Suite	8.9	OS command injection	24 Aug	KEV 21 Aug. Due on the publication date. Only where zimbra-snmp is installed and notifications enabled. Fixed 10.1.20. CERT Polska confirms exploitation. No Shodan label.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	OVERDUE +38, the deepest tracked. Catalogue now records ransomware use as KNOWN, up from Unknown; Resecurity attributes the chain to INC Ransomware. Credentials, sessions and TOTP seeds are stolen, so rebuild rather than patch.
CVE-2026-18577	N-able N-central	8.2	Auth bypass	6 Aug	OVERDUE +18. Vendor wording is a related attack path rather than a Hotfix 1 bypass; Hotfix 2 build 2026.3.1.10 supersedes Hotfix 1. Closes the W34 watch item. Paired CVE-2026-18556 overdue +17, Storm-1175 attribution unchanged since 10 Aug.
CVE-2026-34486	Apache Tomcat	7.5	Missing encryption (fail-open)	7 Aug	OVERDUE +17. Only where clustering is configured with an EncryptInterceptor, which is not the default; the Tribes receiver auto-binds across 4000-4099. Fixed 11.0.21 / 10.1.54 / 9.0.117. 897 in ZA, an exposure count. EPSS 0.8293.

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-72898	Metabase	10.0	SQL injection (unauth)	14 Aug	OVERDUE +10. No new confirmed victim in the window. 109 in ZA. Public PoC since 10 Aug.
CVE-2026-20349	Cisco Secure Firewall ASA and FTD	8.6	Heap inspection (unauth DoS)	14 Aug	OVERDUE +10. Unauthenticated remote reload, availability only. No Shodan product label for this string, so no ZA figure is published and the 373 ASA WebVPN portals in Section 7.2 do not stand in for it. EPSS 0.0102.
CVE-2026-68820	Microsoft Windows AFD for WinSock	7.0	Use-after-free (local EoP)	25 Aug	Due the day after publication, the only tracked item not yet late. Local vector needing existing access; converts any foothold in this edition to SYSTEM. EPSS 0.0033.

Pattern note: the week's distinguishing feature is breadth rather than severity. Nine additions across seven distinct vendors, Microsoft and TrueConf each appearing twice, spanning a Windows network service, a hypervisor management platform, a document collaboration platform, a mail and collaboration server, a video conferencing server, two machine-learning tools and a desktop operating system, is a catalogue week that no single product owner can absorb. Eight of the nine were patched by their vendor before CISA listed them, in one case four months before, so the exposure is created by patch lag rather than by the absence of a fix. One entry changed status among the carryovers rather than the additions, and it matters more than a new listing: SonicWall SMA 1000 CVE-2026-15409 moved from Unknown to KNOWN for ransomware campaign use, matching Resecurity's attribution of the full chain to INC Ransomware,⁴² and it is the deepest overdue item tracked at thirty-eight days. Four carryover rows retire from the table, each because it has nothing new to say: JetBrains TeamCity CVE-2026-63077, overdue by sixteen days with still no published victimology three weeks on;⁴³ Progress LoadMaster CVE-2026-8037, overdue by fourteen with no publicly confirmed compromise of a named organisation and eSentire recording attempts that did not succeed;⁴⁴ Oracle E-Business Suite CVE-2026-46817, overdue by thirty-seven; and Alibaba Fastjson CVE-2026-16723, re-verified against the 21 August catalogue as still absent from it and patched on the 1.x branch since 29 July, which resolves last week's correction. Metabase CVE-2026-72898 stays in the table on exposure movement rather than new victimology, its public exploit code dating from 10 August.⁴⁵ On EPSS, the Windows IKE entry scores 0.7790 and the TrueConf entries score 0.0079 and 0.0097 while being actively chained by a named actor. 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. On N-central, the vendor's own wording settles last week's open question: Hotfix 2, build 2026.3.1.10, supersedes Hotfix 1 in response to a related attack path rather than repairing a bypass.⁴⁶

29. Zero Day Initiative, CVE-2026-33824: remote code execution in Windows IKEv2 (23 April 2026).

<https://www.zerodayinitiative.com/blog/2026/4/22/cve-2026-33824-remote-code-execution-in-windows-ikev2>

30. FIRST, Exploit Prediction Scoring System scores, retrieved 23 August 2026. <https://www.first.org/epss/>

31. QUIRSO GmbH, Global exploitation of CVE-2026-59310 by a suspected Chinese-nexus APT and related CVE-2026-59309 activity (15 August 2026). https://medium.com/@quirso_de/global-exploitation-of-cve-2026-59310-by-suspected-chinese-nexus-apt-related-cve-

2026-59309-443a79e1466d

32. The Hacker News, Attackers exploit Zimbra SNMP flaw for remote code execution (20 August 2026), quoting the CERT Polska bulletin of the same week. <https://thehackernews.com/2026/08/attackers-exploit-zimbra-snmp-flaw-for.html>

33. Kaspersky Securelist, Head Mare delivers PhantomCore and PhantomGraph backdoors via an unpatched TrueConf server (11 August 2026). <https://securelist.com/tr/head-mare-targets-trueconf-server-with-phantomcore/120988/>

34. TrueConf, Security fixes, updates and advisories (published 11 June 2026, modified 12 August 2026). <https://trueconf.com/blog/news/security-fixes-updates-and-advisories>

35. GitHub Security Advisory GHSA-7gwp-5pfp-969j, MLflow server-side request forgery in the model registry webhooks API. <https://github.com/advisories/GHSA-7gwp-5pfp-969j>

36. The Hacker News, Attackers exploit MLflow SSRF flaw to reach cloud metadata services (18 August 2026), reporting watchTower telemetry. <https://thehackernews.com/2026/08/attackers-exploit-mlflow-ssrf-flaw-to.html>

37. Apple, About the security content of macOS Sequoia 15.7.9 (6 August 2026). <https://support.apple.com/en-us/148171>

38. The Hacker News, Apple macOS Screen Sharing flaw exploited to install cryptominers (15 August 2026, updated 18 August 2026). <https://thehackernews.com/2026/08/apple-macos-screen-sharing-flaw.html>

39. Huntress, macOS Screen Sharing RCE patched (7 August 2026). <https://www.huntress.com/blog/macos-screen-sharing-rce-patched>

40. GitHub Security Advisory GHSA-q279-jhrf-cc6v, Ray dashboard code injection via browser-originated requests. <https://github.com/advisories/GHSA-q279-jhrf-cc6v>

41. The Hacker News, CISA flags actively exploited Ray flaw (18 August 2026). <https://thehackernews.com/2026/08/cisa-flags-actively-exploited-ray-flaw.html>

42. Resecurity, From wsproxy to root: INC Ransomware and the SonicWall SMA exploit chain (1 August 2026). <https://www.resecurity.com/blog/article/from-wsproxy-to-root-inc-ransomware-and-sonicwall-sma-exploit-chain>

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

44. eSentire, Progress Kemp LoadMaster vulnerability targeted, CVE-2026-8037 (30 June 2026). <https://www.esentire.com/security-advisories/progress-kemp-loadmaster-vulnerability-targeted-cve-2026-8037>

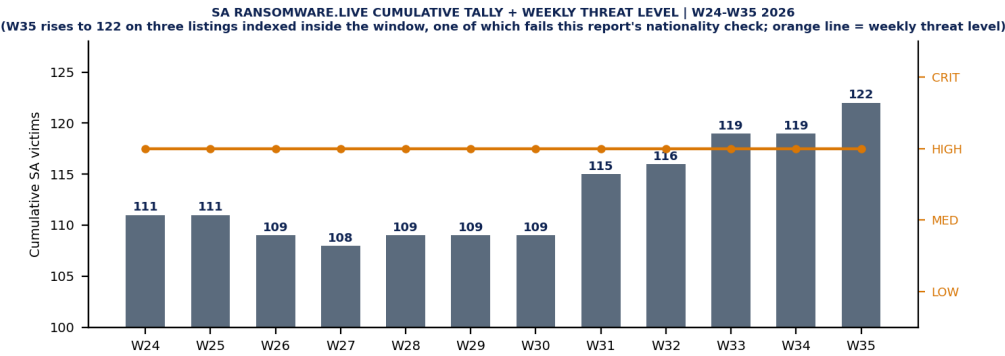
45. Wiz Research, Inside the Metabase SQLi: exploited in the wild (10 August 2026). <https://www.wiz.io/blog/inside-the-metabase-sqli-exploited-in-the-wild>

46. N-able, N-central security update, 10 August 2026 (modified 13 August 2026). <https://www.n-able.com/blog/n-central-security-update-august-10-2026>

6. RANSOMWARE LANDSCAPE

The South African victim feed held 122 records when retrieved at 05:00 UTC on 23 August 2026, up three on the previous week, the collection passing its integrity check: country-scoped by path, 122 records of which 122 were South African, a filter purity of 1.0, clean exit.² All three of the increase carry a discovery date inside the window of 16 to 22 August, so this is new activity rather than a back-fill or a restoration, and no delisting was observed.

One of the three is not South African. Trends And Concepts, listed by Qilin on 20 August, is a Philippine interior fit-out company; the reasoning and the corroborating tracker are in Section 4.3.^{2,12} The cumulative figure of 122 is reported as the feed holds it, because adjusting it unilaterally would make this series incomparable with the source everyone else reads, and because the same error almost certainly sits in the historic tally at a rate nobody has measured. What changes is the derived count: two South African claims this week rather than three, with the KPI table carrying both figures.



Baseline at W34 close	119 cumulative South African records
Movement in window	3 new listings, 0 delistings or restorations observed
End count	122, retrieved 05:00 UTC on 23 August 2026, filter purity 1.0
New listings	The Courier Guy (medusalocker, discovered 16 August), Babcock (thegentlemen, 19 August), Trends And Concepts (qilin, 20 August)
Nationality check	2 of 3 stand. Trends And Concepts is Trends and Concepts Total Interior Solutions of Makati, Philippines, and is counted in the feed total but not in the derived South African claim count
Feed tier	FREE v2, documented as delayed relative to PRO. Figures carry that caveat
Threat-level drivers	Two unresolved leak-site claims against South African organisations; nine KEV additions of which six are overdue at publication; 646 SharePoint and 109 Metabase instances exposed against actively exploited flaws

Group notes: fourteen groups have been active against South Africa in the last 120 days, two more than last week; the additions are medusalocker and qilin, the second of them on the listing ruled non-South-African in Section 4.3.² MedusaLocker has not listed a South African victim before. The Gentlemen has, six times between January and April 2026, so Babcock is a resumption after four months rather than a first appearance. Krybit, which took three South African victims between 2 and 7 August after one victim in the preceding four months, has now been silent for two consecutive windows. The temporal-clustering test set in W33 stays unanswerable, because a group that claims nothing supplies no evidence either way. After two silent weeks the more economical reading is that the burst was one affiliate's scheduling rather than an African campaign; that is offered as the hypothesis a third silent week would strengthen and a new cluster would destroy, not asserted as a finding.

7. OSINT EXPOSURE & ATTACK SURFACE

All figures here are VERIFIED South African exposure counts retrieved at 05:01 UTC on 23 August 2026.⁹ They count instances of a product reachable from the internet, identifiable by fingerprint, and already indexed by Shodan, which scans on its own cycle and does not see everything, so each figure is a floor rather than a census. They are exposure counts: the vulnerability filter is unavailable on this plan, and no figure should be read as "N South African systems vulnerable to CVE-X". Results that failed fingerprint corroboration are held back, and organisation-level facets are never published, because naming a South

African company as running an exposed appliance in a document distributed without restriction is targeting information.

7.1 Three New Panel Entries, All Promoted by This Week's Catalogue Additions

The panel gained three queries this week, each promoted automatically from a catalogue addition and each confirmed against its own product facet before use.⁹ **MLflow** returns 71 South African instances at 100 per cent facet purity, derived from CVE-2026-64849; **Ray** returns 54, from CVE-2025-62593; **VMware vCenter** returns 4, from CVE-2026-59310. The first two are worth pausing on, because together they describe 125 internet-facing machine-learning platform instances in a surface for which this report has not previously carried a South African number. Both default to unauthenticated administrative APIs, both entered the catalogue in the same week, and neither is the kind of system that appears on a register the security team maintains, because data science stands them up. The vCenter figure of 4 is not reassurance: vCenter is normally internal, so the external count is the visible fraction of a larger population, and the flaw is reachable from any internal foothold.

Four products were held back and the reasons are the point of holding them. Zimbra Collaboration Suite, TrueConf Server and Microsoft Internet Key Exchange service extensions produced no Shodan product label across repeated fingerprinting attempts, so no South African figure exists for three of this week's nine additions and none should be inferred from that silence.⁹ Apple macOS returned zero at a facet purity of zero, held rather than published, because a zero is what a wrong fingerprint produces. Two standing queries remain unpublishable: Arista VeloCloud at PROVISIONAL on the same reasoning, and Palo Alto GlobalProtect marked BROKEN because a page-title match returns 4,850 with a top product facet of Microsoft IIS while free text returns zero.

7.2 The Standing Exposure Panel

Microsoft SharePoint on-prem	646, http.component match. Free text returns 2 and is wrong: the component index and banner text are different indexes. Relevant to CVE-2026-55040
Apache Tomcat	897. CVE-2026-34486 is reachable via the Tribes clustering receiver on TCP 4000 rather than the web port, so read this as an exposure count
Metabase	109, up from 84 last week. Ports resolve as 47 on 443, 36 on 3000, 13 on 80 and a tail on 30001 and 444. Port 3000 is the application default and indicates instances stood up without a managed reverse proxy
MLflow	71, new to the panel, promoted from CVE-2026-64849. Facet 100 per cent on the MLflow product family
Ray	54, new to the panel, promoted from CVE-2025-62593. Facet 100 per cent on the Ray product family
VMware vCenter	4, new to the panel, promoted from CVE-2026-59310. An external count of a normally internal system
Exposed RDP (port 3389)	7,767 services, all on 3389, of which 7,167 carry the Remote Desktop Protocol product label. MedusaLocker's documented primary access route

Exposed port 445	4,817 services on that port. Most are unfingerprinted, so read these as services on port 445 rather than as identified SMB servers
Fortinet FortiGate	2,797. Facet resolves cleanly across model variants; free text 'fortigate' independently corroborates
SonicWall, all products	2,845, summing five product strings because Shodan rejects an OR of product filters. Cannot be narrowed to the SMA 1000 line that carries CVE-2026-15409
Others tracked	Cisco ASA WebVPN 373 matched on the /+CSCOE+/ path, WordPress 417 and a floor rather than a total, Citrix Netscaler 103, IBM Langflow 69

Most panel figures are higher than last week, several of them steeply: SharePoint 498 to 646, WordPress 351 to 417, FortiGate 2,493 to 2,797, Metabase 84 to 109, Langflow 42 to 69. Not all moved up, and exposed RDP fell from 7,778 to 7,767.⁹ No conclusion is drawn from any of it, because the collection itself forbids one: the feed 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.⁹ They are point-in-time snapshots of what one scanner had indexed at 05:01 UTC on 23 August, and the right use of them is the absolute magnitude of an exposed population sitting against an actively exploited flaw, which is what Section 7.1 and the Top 3 Actions rely on.

8. REGULATORY & POLICY

8.1 The Regulator's Publication Record, Corrected

Last week's edition stated that the Information Regulator's most recent publication was the enforcement notices of 2 June 2026 and put the silence at eleven weeks. The 2 June item is real: it is a media statement announcing that the Regulator had issued enforcement notices for contraventions of POPIA and PAIA by public and private bodies.⁴⁷ It is not the most recent publication. The Regulator issued an enforcement notice to the Gauteng Department of Health under section 77J of PAIA, on Form H, dated 8 June 2026 and signed by the Chairperson, ordering the release of internal audit reports and a schedule of payments to suppliers of one named hospital between January 2020 and June 2023, to a complainant the notice names as Mr Jeffrey Wicks. Three dates attach to it: 8 June on the instrument, 10 June on the Regulator's own enforcement notices index, and an 11 June server timestamp on the file. This report measures from the instrument date.¹⁴ Measured from 8 June, the interval at last week's publication date of 17 August was ten weeks. The figure printed was eleven. At this edition's publication date of 24 August the interval is eleven weeks, so the number in the KPI table is unchanged from last week only because last week's was a week early.

One caveat cuts against reading too much into regulatory silence. Since 1 April 2025 security compromise notifications reach the Regulator through its eServices portal, and it neither routinely publishes them nor maintains a public breach register, so the absence of a public statement about a breach is not evidence that it was not notified. The narrower statement that can be made is this: the Regulator has issued no public statement, assessment or enforcement notice concerning LEGO Certified Stores South Africa, Toyota South Africa Motors, Euphoria Telecom, DC Partner, Fidelity Services Group or The Courier Guy, and no substantive regulatory output at all for eleven weeks. Procurement and recruitment notices have

continued throughout, including a chief executive advertisement in July and the SSL certificate request of 21 August, so this is silence on breaches rather than an inactive organisation. It does publish and it does enforce, as the June instruments show. The gap is between the volume of South African notification events since June and the volume of public regulatory output over the same period.

8.2 Section 22 When You Have Been Named But Cannot Find Anything

The Courier Guy's position raises a question every South African organisation will eventually face, and the law is worth stating rather than the instinct. Section 22 of POPIA requires notification to the Regulator and to affected data subjects where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person. The trigger is a reasonable belief rather than proof. It is also not a leak-site post: an attacker's claim is not by itself reasonable grounds, or every organisation named by every group would be obliged to notify on the strength of a criminal's marketing.¹

That leaves the assessment with the organisation, and the discipline worth adopting is to write it down while the investigation runs. Three questions carry it. What did the actor specifically claim, and can that be tested against a log that exists. What would this actor's documented tradecraft have left behind, and has anyone looked there. At what point does absence of evidence become evidence of absence, given how long the relevant logs are retained. A company that can answer those three in writing has a defensible position whichever way the finding goes; one that says it has no evidence without having looked has a statement rather than a position, and the Regulator is entitled to probe the difference.

Readers who need the constituency-appropriate first technical contact rather than a compliance destination should use the six South African teams registered with FIRST, which are listed in full with their constituencies and contact details in the W34 edition and remain current in this week's collection.⁴⁸ The Cybersecurity Hub is the national team for private and public sector organisations; ECS-CSIRT at the State Security Agency covers government and military. Identify which one covers you before you need it.

9. WEEKLY THREAT HUNT & IOCs

Six missions. Two P1 cover the ransomware groups that named South African organisations this week and a third the SharePoint token forgery, which pairs public exploit code with the largest South African exposure figure here. Three P2 cover six of the remaining catalogue additions, grouped by where they sit in an estate. Indicators come from vendor advisories, named responder reporting and the per-group indicator and YARA feeds,⁴⁹ including a published YARA rule for the reverse_ssh framework used against vCenter,⁵⁰ and the atomic detail is exported to iocs_w35.csv rather than repeated here.

Two catalogue additions carry no mission and the reasons are stated rather than left to inference. Microsoft Internet Key Exchange service extensions CVE-2026-33824 is the most severe entry in this edition and has no mission because there is nothing to hunt on: neither CISA nor Microsoft has published any detail of the observed attacks, and the only public technical work is Zero Day Initiative's analysis of the flaw itself.^{6,34} That analysis does yield a usable network signature for anyone able to inspect IKE traffic, being a Microsoft Security Realm Vendor ID in an IKE_SA_INIT followed by a fragmented IKE_AUTH from the same source in the same session on UDP 500 or 4500; it is exported to iocs_w35.csv against the Section 10 control rather than dressed up as a mission.³⁴ Apple macOS CVE-2026-65400 is excluded

because Shodan returns zero for macOS in South Africa at zero facet purity, and this report will not build a mission on an unproven fingerprint; its controls are in Section 10. The brand-impersonation activity in Section 3.3 is not a catalogue addition and carries no mission because neither researcher published atomic indicators.

TH-2026-W35-01: MedusaLocker Intrusion, Staging and Pre-Encryption Behaviour	P1 CRITICAL: SA organisation named 16 Aug; 7,767 RDP services exposed in ZA
Hypothesis: An operator has entered through an exposed or weakly configured remote desktop service, or a phishing message carrying the payload directly, and has moved to staging before encryption. The hunt is for the pre-encryption sequence, the window in which the outcome can still be changed, and it runs whether or not the organisation has been named. MITRE ATT&CK: T1133 (External Remote Services), T1566 (Phishing), T1059.001 (PowerShell), T1562.009 (Impair Defenses: Safe Mode Boot), T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery). IOCs: Behavioural, from the FBI and CISA advisory: modification of the EnableLinkedConnections registry value, followed by a LanmanWorkstation service restart; svhost.exe or svhostt.exe in the roaming application data directory with a fifteen-minute scheduled task; a reboot into safe mode; ransom notes in every folder holding encrypted files, filenames including how_to_recover_data.html, READINSTRUCTION.html and !!!HOW_TO_DECRYPT!!!. Nineteen SHA-256 sample hashes, the group Tox contact and the win_medusalocker_auto YARA rule are exported to iocs_w35.csv from the per-group feeds. Data Sources: Windows Security and System event logs, Sysmon registry and process-creation events, scheduled task creation, RDP and VPN authentication, EDR telemetry, and mail-system export and search-audit logs. Detection Guidance: Alert on any write to EnableLinkedConnections outside a change window and treat a LanmanWorkstation restart within minutes of one as high confidence. Enumerate scheduled tasks created since 1 August with a recurrence under an hour. Where the organisation has been named, reconcile the actor's claim against mail export and search-audit logs for the fortnight to 16 August and review remote desktop and VPN authentication over the same period against a known-user list. Record the outcome in writing either way: that record is the section 22 assessment.	

TH-2026-W35-02: The Gentlemen: Group Policy Deployment and Vulnerable Driver Loading**P1 CRITICAL:** SA organisation named 19 Aug; 7th SA victim since January

Hypothesis: An affiliate has obtained domain administrator rights and is preparing or has executed a domain-wide deployment through Group Policy from a domain controller, having first disabled endpoint protection by loading a signed but vulnerable driver. An endpoint-only investigation misses both halves, which is why patch status and a clean EDR console are not sufficient evidence.

MITRE ATT&CK: T1484.001 (Domain Policy Modification: Group Policy Modification), T1021.002 (SMB/Windows Admin Shares), T1543.003 (Windows Service), T1053.005 (Scheduled Task), T1211 and T1068 via BYOVD, T1562.001 (Impair Defenses), T1070.001 (Clear Windows Event Logs), T1490 (Inhibit System Recovery), T1486.

IOCs: deploy_gpo.ps1 in the temporary directory; ransomware executables written to NETLOGON; seven signed drivers loaded for defence evasion, MD5 hashes exported to iocs_w35.csv, being ProcessMonitorDriver.sys, wamsdk.sys, gamedriverx64.sys, biontdrv.sys (two published hashes), inpoutx64.sys, a Topaz anti-fraud driver and Havoc.sys; Windows Kernel Explorer or OpenArk64; scheduled tasks gentlemen_system, UpdateSystem, UpdateUser, DefU, UpdateGU and UpdateGU2 and services DefSvc, UpdateSvc and UpdateSvc2; ransom note README-GENTLEMEN.txt and wallpaper gentlemen.bmp; recon tooling SharpADWS, NetScan and Advanced IP Scanner.

Data Sources: Group Policy object change auditing, SYSVOL and NETLOGON file auditing, domain controller PowerShell script block logging, service and scheduled task creation events, driver load events and Sysmon.

Detection Guidance: Alert on any Group Policy object created or modified outside a change window, on any executable written to NETLOGON, and on the string gentlemen in a scheduled task name. Enable the Microsoft vulnerable driver blocklist and alert on load attempts for the eight published hashes covering those seven drivers rather than only blocking them, because the attempt is the earliest signal available. Correlate wevtutil clearing of the Security log with shadow-copy deletion in the same session.

TH-2026-W35-03: SharePoint CVE-2026-55040: Forged JWT Authentication Bypass**P1 CRITICAL:** public PoC 11 Aug; exploitation 12 to 13 Aug; 646 exposed in ZA

Hypothesis: An unauthenticated attacker has forged a JSON web token that on-premises SharePoint accepts, impersonating a site user or administrator, and is reading or modifying documents with no authentication event that looks like a sign-in.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1606.002 (Forge Web Credentials: SAML and Web Tokens), T1078 (Valid Accounts), T1213.002 (Data from Information Repositories: SharePoint), T1041.

IOCs: Structural rather than atomic. A JSON web token whose outer header declares alg as none and carries no outer signature; an actor token whose x5t header carries the thumbprint of the farm's own security token service certificate; an inner signature that is non-empty but never verifies, a trivial placeholder in the published proof of concept. Enumeration of users by security identifier against the domain controller shortly after such a token is accepted. Affected: SharePoint Enterprise Server 2016 and 2019 and Subscription Edition below the July 2026 update.

Data Sources: SharePoint ULS and audit logs, IIS request logs including the Authorization header where captured, WAF and reverse proxy logs, and domain controller LDAP query logs.

Detection Guidance: Apply the July 2026 update on Monday 24 August; the fix has existed since July and the exposure is patch lag. Where a WAF or proxy logs request headers, alert on any bearer token whose decoded outer header sets alg to none. In ULS logs look for server-to-server token acceptance followed immediately by document enumeration from an address with no prior authenticated session. Treat a match as credential-equivalent and scope by the impersonated account's reach rather than by the SharePoint server.

TH-2026-W35-04: VMware vCenter CVE-2026-59310 and reverse_ssh Persistence**P2 HIGH:** 361 victim IPs across 47 countries by 7 Aug; no workaround, patch only

Hypothesis: An attacker with network access to vCenter, from the internet or an existing internal foothold, has used the Syslog server path traversal to execute code and installed the open-source reverse_ssh framework through a cron job for persistence and outbound command and control.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1053.003 (Scheduled Task/Job: Cron), T1219 (Remote Access Software), T1572 (Protocol Tunneling), T1071.004, T1078.

IOCs: A cron job on the vCenter appliance no administrator created. reverse_ssh client binaries, for which QUIRSO published a generic YARA rule on 10 August; the rule also fires on legitimate reverse_ssh use, so a hit on a vCenter appliance is significant and a hit elsewhere is a question. Outbound SSH from the appliance to an address outside the management network. The responder is withholding network indicators pending law enforcement coordination, so no addresses are published here.

Data Sources: vCenter appliance shell history and cron configuration, appliance and Syslog service logs, and egress netflow and firewall logs from the management network.

Detection Guidance: Patch to 9.1.0.0300, 9.0.2.0100, 8.0 U3k or 8.0 U2f by branch; there is no workaround. Treat outbound SSH from a vCenter appliance as an alert with no benign baseline in most estates, and compare cron entries against a known-good build. If the appliance was internet-reachable at any point since 29 July, rebuild rather than clean, because code execution on vCenter reaches every guest it manages.

TH-2026-W35-05: Zimbra and TrueConf: Two Mail and Conferencing Servers Under Active Attack**P2 HIGH:** Zimbra due 24 Aug, TrueConf overdue +1; named APT on the TrueConf chain

Hypothesis: An unauthenticated attacker has executed operating system commands on a Zimbra server through SNMP notification processing, or chained the two TrueConf flaws over TCP 4307 to reach SYSTEM and replace the client installer with a trojanised build. The second case matters even where neither product is run, because a partner's compromised TrueConf server serves malicious installers to your staff.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1195.002 (Supply Chain Compromise: Software Supply Chain), T1543.003 (Windows Service), T1102 and T1567.002 (Web Service and Cloud Storage for C2), T1070.001.

IOCs: Zimbra, per CERT Polska: unexpected Zimbra service restarts in /var/log/zimbra.log, and files created in the last thirty days under /opt/zimbra/jetty/webapps/, /opt/zimbra/jetty_base/webapps/ and /tmp/. TrueConf, per Kaspersky: a PHP web shell replacing locale.php in the server's public JavaScript directory, MD5 4d27b4eb1c5dbb3d8160f29b8119523e, YARA rule apt_HeadMare_FakeLocale_webshell; a trojanised installer trueconf_windows_update.exe, MD5 748c9f8cb1065000616204935f96207f; Windows services SysExcSvc and SysReadSvc; and five command and control addresses. All are exported to iocs_w35.csv.

Data Sources: Zimbra service and web server logs, Linux file integrity monitoring, Windows service creation events, EDR file-write telemetry on TrueConf servers, perimeter logs for TCP 4307, and egress logs for Microsoft Graph and OneDrive traffic originating from servers.

Detection Guidance: On Zimbra, remove the zimbra-snmppackage if it is not needed, which removes the vulnerable code path entirely, otherwise upgrade to 10.1.20. On TrueConf, upgrade to 5.3.9, 5.4.9 or 5.5.5 and block TCP 4307 at the perimeter, because it is open by default. Verify the signature of any TrueConf client installer before deployment, the malicious distributions having carried none. Hunt the five addresses across sixty days of perimeter logs.

TH-2026-W35-06: MLflow and Ray: Unauthenticated Machine-Learning Platform APIs**P2 HIGH: 71 MLflow and 54 Ray instances exposed in ZA; both added to KEV this week**

Hypothesis: A machine-learning platform stood up by a data science team, outside the register the security team maintains, is exposing an unauthenticated administrative API to the internet. On MLflow the attacker uses the webhook test endpoint as a full-read server-side request forgery to reach cloud metadata and take instance credentials; on Ray the attacker submits a job that executes shell commands, reachable from a developer's browser.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1552.005 (Cloud Instance Metadata API), T1078.004 (Cloud Accounts), T1059.004, T1610, T1496 (Resource Hijacking).

IOCs: MLflow: POST to /api/2.0/mlflow/webhooks and /api/2.0/mlflow/webhooks/{id}/test; the published proof of concept redirects to <http://169.254.169.254/latest/meta-data/iam/security-credentials/>; any outbound request from an MLflow server to a link-local, loopback or RFC1918 address. Affected below 3.15.0. Ray: POST to /api/jobs/ and /api/job_agent/jobs/ on port 8265 with a non-browser User-Agent, the proof of concept using the literal value Other with source metadata nccgroup/singularity and a shell command in the endpoint field. Affected below 2.52.0.

Data Sources: Application logs for both platforms, reverse proxy and ingress logs, cloud metadata service access logs and audit trails, egress netflow from data science subnets, and cloud billing anomaly alerts.

Detection Guidance: First find them: query cloud accounts for anything listening on 5000 or 8265 or a load balancer fronting either, and ask the data science function directly, because these systems are usually not on the security register. Upgrade MLflow to 3.15.0 and Ray to 2.52.0. Enable Instance Metadata Service version 2 on any MLflow host, which defeats the SSRF path even unpatched, put authentication in front of the Ray dashboard and take it off internet-facing interfaces, and rotate any instance credential used from an unexpected address.

47. Information Regulator of South Africa, media statement: Regulator issues enforcement notices for the contraventions of POPIA and PAIA by public and private bodies (2 June 2026). <https://infoeregulator.org.za/wp-content/uploads/2026/06/MEDIA-STATEMENT-INFORMATION-REGULATOR-ISSUES-ENFORCEMENT-NOTICES-FOR-THE-CONTRAVENTIONS-OF-POPIA-AND-PAIA-BY-PUBLIC-AND-PRIVATE-BODIES.pdf>

48. FIRST, member teams directory. South African CSIRT records retrieved through the ransomware.live /csirt/ZA endpoint on 23 August 2026, six teams. <https://www.first.org/members/teams/>

49. ransomware.live, per-group atomic indicator and YARA endpoints, retrieved 23 August 2026. <https://www.ransomware.live/>

50. QUIRSO GmbH, generic YARA rule for reverse_ssh client binaries, 10 August 2026. https://github.com/QUIRSO/QTRDetectionContent/blob/main/2026-08-10_reverse_ssh_generic.yar

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. Take the nine catalogue additions as an inventory exercise before taking them as a patching exercise.

On Monday 24 August, answer one question for each of the nine products: do we run it, where, and who owns it. The three most likely to fail that question are MLflow, Ray and vCenter, the first two because data science teams stand them up outside the security register and the third because it sits in an infrastructure team's estate rather than an application owner's. Then patch in deadline order: Ray to 2.52.0, Windows to the April 2026 or later cumulative update, vCenter to 9.1.0.0300, 9.0.2.0100, 8.0 U3k or 8.0 U2f, SharePoint to the July 2026 update, macOS to 26.6.1, 15.7.9 or 14.8.9, TrueConf to 5.3.9, 5.4.9 or 5.5.5, and Zimbra to 10.1.20. Where patching cannot be immediate, the network controls are cheap: block inbound UDP 500 and 4500 on hosts that do not terminate IPsec, TCP 4307 to TrueConf, TCP 5900 to any Mac, and TCP 8265 to Ray. On macOS specifically, where no South African exposure figure exists and the observed

outcome is root access and a Monero miner, the control is the 6 August update plus an unconditional perimeter block on 5900.

2. Hunt the two named actors on behalf of organisations that have not been named. The Group Policy and NETLOGON checks in TH-2026-W35-02 and the registry and scheduled-task checks in TH-2026-W35-01 are estate-wide hunts costing a query each, and each returns either a finding or a clean result that means something. Enable the Microsoft vulnerable driver blocklist and alert on load attempts rather than only blocking them: for a bring-your-own-vulnerable-driver actor the attempt is the earliest signal available and it precedes the encryptor.

3. Treat the exposure figures here as a floor and measure your own. The Section 7 panel counts only what one scanner had already indexed at a single moment, and the feed itself warns that individual counts have moved by as much as 73 per cent inside a day, so no organisation should manage to these numbers. Run the equivalent queries against your own address space on your own schedule and reconcile the result against the asset register. The gap between those two lists is the finding, and it is the same gap that puts an MLflow instance on the internet.

Management (CISO / Board)

1. Decide in advance how the organisation responds to being named on a leak site. Two South African companies were named this week and neither has acknowledged a compromise. It will happen to more of them, and when it does the organisation has hours rather than days to say something to customers, staff and journalists. Agree now who owns the statement, what it may say before the investigation concludes, and what evidentiary threshold moves the organisation from an unverified claim to a POPIA section 22 notification. Section 8.2 sets out the legal trigger, which is reasonable grounds to believe rather than proof.

2. Ask for the inventory answer rather than the patching answer. The question worth asking after a week like this is not whether the nine vulnerabilities have been patched. It is how long it took to establish which of the nine products the organisation runs. If that took more than a day the constraint is asset management rather than patching capacity, and the next catalogue week will produce the same delay. It is measurable and belongs on a dashboard: time from catalogue publication to a confirmed answer on whether the organisation is affected.

3. Price fraud alongside breach. Absa disclosed a R129 million increase in operational risk losses attributed largely to digital fraud over six months, against a technology budget of R8.8 billion and mature countermeasures. Most South African organisations report fraud and cyber through separate channels to separate committees, which makes the combined exposure invisible at board level. Ask for one view of loss from social engineering, account takeover and impersonation of the organisation's own brand, and read it beside the breach register rather than instead of it.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 18th CONSECUTIVE WEEK

The South African cyber threat level remains HIGH for an eighteenth consecutive week (16 August to 22 August 2026). De-escalation to MEDIUM was considered on the ground that no South African organisation confirmed a breach in this window, and rejected: two are under unresolved extortion claims, nine vulnerabilities entered the catalogue of which six are overdue at publication, and four of those affect products with counted South African exposure, including 646 SharePoint instances against a flaw with public exploit code. Escalation to CRITICAL was not close: no national-scale event, no systemically important institution out of service, no dataset published, and the week's only victim-confirmed figure is a financial loss disclosure rather than an operational compromise.

Rationale

- **Two unresolved leak-site claims against South African organisations.** MedusaLocker named the country's largest express parcel courier on 16 August, its first South African listing, and The Gentlemen named the South African arm of an engineering and defence support group on 19 August, its seventh since January and its first in four months. Neither organisation has acknowledged a compromise and neither claim is corroborated, so both are CLAIMED.
- **Nine catalogue additions in five days, six overdue at publication.** The set spans seven distinct vendors and reaches a Windows network service, a hypervisor management platform, a document collaboration platform, a mail and collaboration server, a video conferencing server, two machine-learning tools and a desktop operating system. Eight had a vendor fix before CISA listed them, in the Windows case four months before, so the residual exposure is patch lag. vCenter CVE-2026-59310 had 361 victim addresses across 47 countries by 7 August; SharePoint CVE-2026-55040 had a working proof of concept on 11 August and reported exploitation with it within two days against 646 exposed South African instances; Ray and MLflow were both scanned within hours of their identifiers being assigned.
- **Fraud losses that a victim organisation has quantified.** Absa recorded a R129 million increase in operational risk losses to R369 million for the half year, attributed largely to social engineering and malicious applications on customer devices, alongside vendor reporting of Android trojans impersonating four South African brands with SMS one-time-password interception as the core capability.
- **Against escalation, stated plainly: nothing was confirmed.** No South African organisation confirmed a breach this window, no dataset was published, no operational disruption was reported, and one of the three apparent South African listings turned out to be a Philippine company. The domestic evidence base is thinner than the threat level implies, and the level is held on the vulnerability picture rather than the incident picture.

Next-Week Watch (W36)

- **The Courier Guy's investigation.** Whether the company's position changes, whether MedusaLocker publishes files rather than filenames, and whether the Information Regulator is notified. The observation that separates a real extraction from a fabricated listing is the publication of content that the company can recognise; a price that drops or a listing that disappears without payment points the other way.
- **Babcock, and which Babcock.** Whether either the South African business or the parent group makes a statement and whether a dataset appears. If the parent responds, note whether it accepts the claim as against the African business or disputes the attribution, because that is the question the leak post leaves open.
- **Whether a stable exposure baseline can be established at all.** Most panel figures rose this week and exposed RDP fell, and the feed's own caveat is that rescan artefacts have moved individual counts by up to 73 per cent inside a day, so week-on-week movement cannot currently be read as anything. The observation that would change that is a run of three or four collections in which a given product family varies by only a few per cent; until a figure is stable enough to have a trend, this report will publish these counts as point-in-time magnitudes and draw no movement conclusions from them.
- **Marsello, and the Information Regulator now on six named organisations.** Marsello has still published nothing of its own and no second South African brand has notified, so what separates a single-brand event from a multi-brand one remains a second section 22 notice naming it. The corrected regulatory clock stands at eleven weeks with no publication of any kind; watch for any statement, assessment or enforcement notice naming LEGO Certified Stores, Toyota South Africa Motors, Euphoria Telecom, DC Partner, Fidelity Services Group or The Courier Guy, remembering that eServices notifications are not published, so silence is not evidence that nothing was filed.
- **Two items closed this week, recorded so they are not carried by habit.** The N-able question, whether Hotfix 1 was bypassed or a second path found, is answered: the vendor's wording is a related attack path and Hotfix 2 build 2026.3.1.10 supersedes rather than repairs Hotfix 1. The W34 aggregator map discrepancy is superseded, because the nationality check introduced this week tests record content rather than record count.
- **Krybit, Toyota's SMS provider, and the open South African listings.** Krybit has been silent for two windows and a third would strengthen the reading that the early-August burst was one affiliate's workload. Toyota's bulk SMS provider is still unnamed, which keeps that incident unactionable for every other South African organisation. DC Partner, Buzz Trading 104 and Serengeti Estates remain CLAIMED with no dataset surfaced.

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 23 August 2026. **Collection notes.** The feed run completed at 05:04 UTC on 23 August 2026 and passed its integrity check with a clean exit; ransomware.live returned 122 records of which 122 were South African, a filter purity of 1.0. Four Shodan queries were held back and are named in Section 7.1, three for the absence of any product label and one for a zero a second method has not confirmed; two standing queries remain unpublishable. **Environment**

limitations. cisa.gov returns an empty body here, so entries 15 and 23 are the identical advisories from the FBI IC3 mirror, IC3 being a co-authoring agency rather than a third-party rehost, and every KEV date in this edition comes from the locally retrieved catalogue file. The Information Regulator's index pages are accordions this environment cannot render; entry 14 was located through the site's own file directory, which lists every uploaded document with a server timestamp, and the notice itself was then retrieved and read. The Kaspersky ICS-CERT report on the TrueConf campaign could not be retrieved, so entry 31 is the company's own Securelist publication of the same investigation, one day earlier. **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; readers who want the full story should follow the credit link and read it at the source. **Single-source disclosure.** Three sets of facts rest on one South African publication because no other account could be found: The Courier Guy's response to the MedusaLocker claim, including its position on notification and the stated sale price; the Absa loss figures as reported from the interim results; and the Toyota statement of 12 August. A fourth was reclassified during fact-checking: the LEGO Certified Stores story was carried by a second South African publication on 17 August, but that account credits and links the original reporting and adds nothing independent, so it remains single-sourced. On Absa, the operational risk loss figures of R369 million and R240 million sit in the risk-management section of the results booklet, which this environment could not retrieve; they are confirmed through two national outlets rather than read at the primary, and the R129 million delta is arithmetic on those two figures rather than a line Absa printed. **Claims deliberately excluded.** An attribution of the Windows IKE exploitation to a named state-linked actor circulated during this collection and is not repeated, because it could not be traced to any source carrying it and the primary reporting states that neither CISA nor Microsoft has released attack details. A figure for people affected attached to the Trends And Concepts listing by one aggregator is excluded for the same reason: the actor never published it. A report reached this desk during fact-checking that Babcock Africa had published a statement on its own website on 18 August acknowledging a cyber security event. It could not be verified: the site's article pages are client-side rendered and return no text to this environment, no search index carries the item, and no independent coverage exists. It is therefore not used, the incident stays at CLAIMED, and the question is carried into Next-Week Watch for someone with a browser to settle. **Post-publication fact-check.** This edition was re-verified against primary sources after its first build. The material corrections made before delivery were: the VMware vCenter attribution position, which had moved on 15 August and is now carried in full; the Ray proof-of-concept metadata string in the companion indicator file, which was exported with the correct spelling rather than the misspelling the exploit actually uses; the SharePoint chain, which has four weaknesses rather than three; the TrueConf scores, which needed their CVSS version labelled; and several attributions in Sections 3, 4 and 8 where a finding had been credited to the wrong party.

1. 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>
2. ransomware.live, South African victim records, endpoint /v2/countryvictims/ZA, 122 records at filter purity 1.0, retrieved 05:00 UTC on 23 August 2026. <https://www.ransomware.live/>
3. ransomware.live, MedusaLocker group leak-site index, retrieved 23 August 2026. <https://www.ransomware.live/group/medusalocker>
4. CISA, Known Exploited Vulnerabilities catalogue, catalogVersion 2026.08.21, released 21 August 2026, retrieved 23 August 2026. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
5. NVD CVSS base scores with scoring source, retrieved 23 August 2026. <https://nvd.nist.gov/>
6. BleepingComputer, CISA: Critical Windows IKE extension flaw now exploited in attacks (19 August 2026). <https://www.bleepingcomputer.com/news/security/cisa-critical-windows-ike-extension-flaw-now-exploited-in-attacks/>
7. BleepingComputer, Critical VMware vCenter RCE flaw exploited for reverse SSH access (13 August 2026). <https://www.bleepingcomputer.com/news/security/critical-vmware-vcenter-rce-flaw-exploited-for-reverse-ssh-access/>
8. QUIRSO GmbH, Active exploitation of CVE-2026-59310: 361 victim IPs across 47 countries (August 2026). https://medium.com/@quirso_de/active-exploitation-of-cve-2026-59310-361-victim-ips-across-47-countries-9783187cc6ff
9. Shodan country:ZA exposure panel, VERIFIED results only, retrieved 05:01 UTC on 23 August 2026. <https://www.shodan.io/search?query=country%3AZA>

10. The Hacker News, Attackers exploit SharePoint authentication bypass (13 August 2026). <https://thehackernews.com/2026/08/attackers-exploit-sharepoint.html>
11. Rapid7, Microsoft SharePoint JWT token authentication bypass, CVE-2026-55040 (11 August 2026). <https://www.rapid7.com/blog/post/ra-microsoft-sharepoint-jwt-token-authentication-bypass-cve-2026-55040/>
12. Breachsense, Trends and Concepts Total Interior Solutions data breach record, retrieved 23 August 2026. <https://www.breachsense.com/breaches/trends-and-concepts-total-interior-solutions-data-breach/>
13. Breachsense, Babcock International Group – Africa data breach record, discovered 20 August 2026, retrieved 23 August 2026. <https://www.breachsense.com/breaches/babcock-international-group-africa-data-breach/>
14. Information Regulator of South Africa, Gauteng Department of Health enforcement notice, PAIA section 77J Form H, dated 8 June 2026. <https://infoeregulator.org.za/wp-content/uploads/2026/06/GAUTENG-DEPARTMENT-OF-HEALTH-ENFORCEMENT-NOTICE-080626.pdf>
15. FBI, CISA, Department of the Treasury and FinCEN, #StopRansomware: MedusaLocker, product AA22-181A (30 June 2022), retrieved from the FBI IC3 mirror because cisa.gov returns an empty body to this environment. <https://www.ic3.gov/CSA/2022/220630.pdf>
16. Kaspersky Securelist, The Gentlemen RaaS: rapid growth and a new ransomware variant (29 June 2026). <https://securelist.com/the-gentlemen-raas/120447/>
17. Palo Alto Networks Unit 42, No manners here: the ruthless rise of The Gentlemen ransomware (10 July 2026). <https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/>
18. MyBroadband, Major bank in South Africa takes R129-million cyber fraud hit (20 August 2026). <https://mybroadband.co.za/news/security/663249-major-bank-in-south-africa-takes-r129-million-cyber-fraud-hit.html>
19. MyBroadband, DStv, Takealot and South African Airways impersonated to take over bank accounts in South Africa (20 August 2026), reporting NordVPN and Kaspersky research. <https://mybroadband.co.za/news/security/663273-dstv-takealot-and-south-african-airways-impersonated-to-take-over-bank-accounts-in-south-africa.html>
20. MyBroadband, Criminals targeting people who shop online in South Africa (19 August 2026), reporting ESET analysis. <https://mybroadband.co.za/news/security/661906-criminals-targeting-people-who-shop-online-in-south-africa.html>
21. The Citizen, Zero-day hack exposes Lego Certified Stores SA customer data (17 August 2026). <https://www.citizen.co.za/lifestyle/technology/zero-day-hack-exposes-lego-certified-stores-sa-customer-data/>
22. 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>
23. FBI, CISA and HHS, #StopRansomware: Medusa ransomware, product AA25-071A, originally published 12 March 2025, last updated 18 August 2026, retrieved from the FBI IC3 mirror. <https://www.ic3.gov/CSA/2026/260818.pdf>
24. American Hospital Association, Agencies issue update on Medusa ransomware activity (19 August 2026). <https://www.aha.org/news/headline/2026-08-19-agencies-issue-update-medusa-ransomware-activity>
25. Microsoft Threat Intelligence, The Gentlemen ransomware: dissecting a self-propagating Go encryptor (28 May 2026). <https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/>
26. ransomware.live, group statistics and per-group victim records, 778 victims recorded for The Gentlemen, retrieved with the 05:00 UTC collection run of 23 August 2026. <https://www.ransomware.live/groupstats/thegentlemen>
27. Cyble, Annual Threat Landscape Report 2025 (copyright 2026 Cyble Inc.), obtained by completing the publisher's registration. Not linkable without registration.
28. Trend Micro, Agenda ransomware uses Rust to target more vital industries (16 December 2022). https://www.trendmicro.com/en_us/research/22/1/agenda-ransomware-uses-rust-to-target-more-vital-industries.html
29. Zero Day Initiative, CVE-2026-33824: remote code execution in Windows IKEv2 (23 April 2026). <https://www.zerodayinitiative.com/blog/2026/4/22/cve-2026-33824-remote-code-execution-in-windows-ikev2>
30. FIRST, Exploit Prediction Scoring System scores, retrieved 23 August 2026. <https://www.first.org/epss/>
31. QUIRSO GmbH, Global exploitation of CVE-2026-59310 by a suspected Chinese-nexus APT and related CVE-2026-59309 activity (15 August 2026). https://medium.com/@quirso_de/global-exploitation-of-cve-2026-59310-by-suspected-chinese-nexus-apt-related-cve-2026-59309-443a79e1466d
32. The Hacker News, Attackers exploit Zimbra SNMP flaw for remote code execution (20 August 2026), quoting the CERT Polska bulletin of the same week. <https://thehackernews.com/2026/08/attackers-exploit-zimbra-snmp-flaw-for.html>
33. Kaspersky Securelist, Head Mare delivers PhantomCore and PhantomGraph backdoors via an unpatched TrueConf server (11 August 2026). <https://securelist.com/tr/head-mare-targets-trueconf-server-with-phantomcore/120988/>
34. TrueConf, Security fixes, updates and advisories (published 11 June 2026, modified 12 August 2026). <https://trueconf.com/blog/news/security-fixes-updates-and-advisories>
35. GitHub Security Advisory GHSA-7gwp-5pfp-969j, MLflow server-side request forgery in the model registry webhooks API. <https://github.com/advisories/GHSA-7gwp-5pfp-969j>
36. The Hacker News, Attackers exploit MLflow SSRF flaw to reach cloud metadata services (18 August 2026), reporting watchTower telemetry. <https://thehackernews.com/2026/08/attackers-exploit-mlflow-ssrf-flaw-to.html>
37. Apple, About the security content of macOS Sequoia 15.7.9 (6 August 2026). <https://support.apple.com/en-us/148171>
38. The Hacker News, Apple macOS Screen Sharing flaw exploited to install cryptominers (15 August 2026, updated 18 August 2026). <https://thehackernews.com/2026/08/apple-macos-screen-sharing-flaw.html>
39. Huntress, macOS Screen Sharing RCE patched (7 August 2026). <https://www.huntress.com/blog/macOS-screen-sharing-rce-patched>
40. GitHub Security Advisory GHSA-q279-jhrf-cc6v, Ray dashboard code injection via browser-originated requests. <https://github.com/advisories/GHSA-q279-jhrf-cc6v>
41. The Hacker News, CISA flags actively exploited Ray flaw (18 August 2026). <https://thehackernews.com/2026/08/cisa-flags-actively-exploited-ray-flaw.html>
42. Resecurity, From wsproxy to root: INC Ransomware and the SonicWall SMA exploit chain (1 August 2026). <https://www.resecurity.com/blog/article/from-wsproxy-to-root-inc-ransomware-and-sonicwall-sma-exploit-chain>
43. JetBrains, CVE-2026-63077 update (7 August 2026). <https://blog.jetbrains.com/teamcity/2026/08/cve-2026-63077-update/>
44. eSentire, Progress Kemp LoadMaster vulnerability targeted, CVE-2026-8037 (30 June 2026). <https://www.esentire.com/security-advisories/progress-kemp-loadmaster-vulnerability-targeted-cve-2026-8037>
45. Wiz Research, Inside the Metabase SQLi: exploited in the wild (10 August 2026). <https://www.wiz.io/blog/inside-the-metabase-sqli-exploited-in-the-wild>
46. N-able, N-central security update, 10 August 2026 (modified 13 August 2026). <https://www.n-able.com/blog/n-central-security-update-august-10-2026>
47. Information Regulator of South Africa, media statement: Regulator issues enforcement notices for the contraventions of POPIA and PAIA by public and private bodies (2 June 2026). <https://infoeregulator.org.za/wp-content/uploads/2026/06/MEDIA-STATEMENT-INFORMATION-REGULATOR-ISSUES-ENFORCEMENT-NOTICES-FOR-THE-CONTRAVENTIONS-OF-POPIA-AND-PAIA-BY-PUBLIC-AND-PRIVATE-BODIES.pdf>

48. FIRST, member teams directory. South African CSIRT records retrieved through the ransomware.live /csirt/ZA endpoint on 23 August 2026, six teams. <https://www.first.org/members/teams/>

49. ransomware.live, per-group atomic indicator and YARA endpoints, retrieved 23 August 2026. <https://www.ransomware.live/>

50. QUIRSO GmbH, generic YARA rule for reverse_ssh client binaries, 10 August 2026.
https://github.com/QUIRSO/QTRDetectionContent/blob/main/2026-08-10_reverse_ssh_generic.yar

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.