



SOUTH AFRICA CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief -- Week 29 | 5 July - 12 July 2026

THREAT LEVEL: HIGH

TLP:WHITE

Prepared by Digital Progression | dpcyber.co.za

Report ID: DP-CTI-2026-W29 | Classification: TLP:WHITE

Published Monday 13 July 2026

(c) 2026 Digital Progression | dpcyber.co.za

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W29)
- 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

1. EXECUTIVE SUMMARY

Overall Threat Level: HIGH (unchanged, 9th consecutive week) -- Week 29 (5 July - 12 July 2026)

Story 1 -- Six KEV Additions in Seven Days, All CVSS 9.8 or Higher, All on a Three-Day Clock -- and Four of Them Are Joomla Website Extensions: CISA added six actively exploited vulnerabilities between 5 and 12 July: Adobe ColdFusion CVE-2026-48282 (CVSS 10.0, path traversal to unauthenticated RCE, exploited less than two hours after disclosure), JoomShaper SP Page Builder CVE-2026-48908 (10.0, exploited as a zero-day), Joomla! Page Builder CK CVE-2026-56290 (10.0), Langflow CVE-2026-55255 (9.9), iCagenda CVE-2026-48939 (9.8) and Balbooa Forms CVE-2026-56291 (9.8).¹²³⁴ Every entry carries a roughly three-day federal remediation deadline under BOD 26-04 rather than the old three-week BOD 22-01 clock: the 7 July batch was due 10 July, the 10 July batch is due 13 July.⁵ Four of the six are third-party Joomla extension file-upload flaws -- exactly the stack that sits under a large share of South African SME, NGO and municipal websites. CONFIRMED.

Story 2 -- South Africa's Breach Bill Goes Public: 3,219 Notifications, R141.96bn, 1.81% of GDP: Analysis published on 6 and 7 July puts 3,219 breaches reported to the Information Regulator in the 2025/26 financial year -- about 268 a month -- at an estimated R141.96 billion of economic drag, or 1.81% of a R7.86 trillion GDP, using the IBM Cost of a Data Breach 2025 South African average of R44.1 million per breach.¹¹¹² The Regulator's own last published figures were 2,374 notifications in 2024/25 and 1,947 between April and November 2025, a 40% year-on-year rise.¹⁵¹³ The R44.1m average breach cost dwarfs POPIA's R10m maximum administrative fine, and the Regulator has published nothing since 2 June.¹⁴¹⁶ CONFIRMED (figures as published); PROBABLE (the 3,219 total is reported by a vendor analysis, not an Information Regulator publication we could retrieve).

Story 3 -- A Sixth Quiet Week on SA Leak Sites, and the Only SA Enforcement Action Is a Telecoms Fraud Penalty: The ransomware.live South Africa tally held at 109, unchanged from W28, with no new SA victim posted in the window -- a sixth consecutive week with no confirmed new SA leak-site listing.²⁰²¹²² The week's only concrete SA regulatory action came from ICASA, which on 9 July confirmed a R6 million penalty against Session Telecoms following an MTN complaint alleging CLI manipulation, call refiling and SIM-boxing, with cease-and-desist orders, withdrawal of numbering resources and 24 months of monthly compliance reporting; the operator is taking the finding on review.¹⁷¹⁸ Globally, INTERPOL's Operation First Light 2026 produced 5,811 arrests and USD 293 million intercepted across 97 countries.²⁴²⁵ CONFIRMED.

KPI Dashboard

Metric	Current (W29)	Prior (W28)	Change	Direction
SA threat level	HIGH	HIGH	Unchanged (9th consecutive week)	FLAT

Metric	Current (W29)	Prior (W28)	Change	Direction
SA ransomware.live victims (total)	109 (verified 12 Jul)	109	No change; no new SA postings	FLAT
New SA RW listings this week (ransomware.live)	0 confirmed	0	6th consecutive quiet week	FLAT
New CISA KEV additions (5 - 12 Jul)	6 (4 on 7 Jul; 2 on 10 Jul)	2 (W28)	Volume tripled; all CVSS 9.8-10.0	UP
KEV remediation clock	~3 days (BOD 26-04)	3 - 8 days observed	Short fuses now the standing norm	FLAT
Joomla third-party extension KEV adds	4 of 6 new adds (SPPB, Page Builder CK, iCagenda, Balbooa)	0	NEW W29 -- CMS supply chain	UP
Highest-severity in-window CVE	Adobe ColdFusion CVE-2026-48282 (CVSS 10.0; exploited <2h post-disclosure)	Oracle EBS CVE-2026-46817 (9.8)	NEW W29	UP
Oracle EBS Payments CVE-2026-46817	Still NOT in KEV; exploited since 27 Jun (day 15)	Exploited ITW; not in KEV	UNCHANGED -- gap widening	FLAT
SA breach notifications (FY2025/26, as published)	3,219 (~268/month); est. R141.96bn / 1.81% of GDP	N/A	NEW W29 -- first public FY total	UP
Information Regulator public activity	Silent; nothing published after 2 Jun 2026	Silent since 2 Jun	NO CHANGE	FLAT
IR s.59 notices -- TransUnion SA + Experian SA	Responses were due ~6 Jul; still no public development	Pending	PENDING (2nd week)	FLAT
SA regulatory enforcement	ICASA: R6m penalty on Session Telecoms (SIM-boxing / CLI manipulation), 9 Jul	None	NEW W29	UP
Global law enforcement	INTERPOL Operation First Light 2026: 5,811 arrests, USD 293m intercepted	Scattered Spider extradition	SUSTAINED PRESSURE	UP
Pick n Pay / Capitec, Profmed / PPSHA (carryovers)	No development 5 - 12 Jul; no PPSHA scope expansion	Capitec card replacements; PPSHA identified	QUIET	FLAT
AVBOB Mutual Assurance (carryover)	~6 weeks post-incident; still no leak-site claim or attribution	Undetermined	UNDETERMINED	FLAT

W29 KEY FRAMING: The domestic incident ledger was empty for a sixth straight week, but the exploitation tempo outside it tripled. Six KEV additions in seven days, every one rated 9.8 or above, every one on a roughly three-day remediation clock, and four of them in the Joomla extension ecosystem -- the

content-management stack that quietly runs a large share of South African SME, NGO and municipal websites that nobody has patched since the site went live. The exposure this week is not the SOC's servers; it is the brochure website that marketing outsourced in 2019. Meanwhile the published cost of South African breaches -- R141.96 billion, 1.81% of GDP, R44.1 million per breach -- landed in the business press while the Information Regulator itself has published nothing since 2 June.

TOP 3 ACTIONS THIS WEEK

1. INVENTORY AND PATCH EVERY JOOMLA SITE YOU OWN, INCLUDING THE ONES YOU FORGOT:

Four of the six new KEV entries are unauthenticated or trivially authenticated file-upload flaws in Joomla third-party extensions -- SP Page Builder (fix 6.6.2+), Page Builder CK (fix 3.6.0), iCagenda and Balbooa Forms. Exploitation of Page Builder CK began on 27 June, hours after the fix shipped, and SP Page Builder was hit as a zero-day. Enumerate every .co.za and .gov.za property your organisation owns or sponsors, identify the CMS and installed extensions, patch or remove, then hunt for web shells (a confirmed artefact is /media/com_pagebuilderck/gfonts/bhup.php) and for newly created Super User accounts.¹²³

2. TREAT ADOBE COLD FUSION AS COMPROMISED UNTIL PROVEN OTHERWISE: CVE-2026-48282 (CVSS 10.0) is a path traversal in the RDS FILEIO handler giving unauthenticated arbitrary file write and RCE on ColdFusion 2025.9, 2023.20 and earlier. It was exploited within two hours of public disclosure and the KEV deadline (10 July) has already lapsed. Apply the 30 June Adobe update, disable RDS in production, and if the server was internet-facing and unpatched between 30 June and 7 July, run a compromise assessment rather than assuming the patch closed the door.¹⁴

3. CLOSE THE UNLISTED-BUT-EXPLOITED GAP: ORACLE EBS AND GITEA: Oracle E-Business Suite Payments CVE-2026-46817 (CVSS 9.8) has now been exploited in the wild for over two weeks and is still not in the KEV catalogue -- the catalogue is a floor, not a work queue. Separately, Gitea CVE-2026-20896 (CVSS 9.8) is under active exploitation: official Docker images at or below 1.26.2 ship with REVERSE_PROXY_TRUSTED_PROXIES set to a wildcard, so any source IP can send an X-WEBAUTH-USER header and authenticate as any user including an administrator, exposing source code and CI secrets. Upgrade to 1.26.3 or 1.26.4, restrict trusted proxies, and rotate repository secrets.⁶

1. Security Affairs -- U.S. CISA adds Adobe ColdFusion, Joomla Page Builder, Langflow, and JoomShaper SP Page Builder flaws to its Known Exploited Vulnerabilities catalog (7 July 2026) -- <https://securityaffairs.com/194927/hacking/u-s-cisa-adds-adobe-coldfusion-joomla-page-builder-langflow-and-joomshaper-sp-page-builder-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

2. The Hacker News -- CISA adds 4 actively exploited Adobe ColdFusion and Joomla extension flaws to KEV catalog (7 July 2026) -- <https://thehackernews.com/2026/07/cisa-adds-4-actively-exploited-adobe.html>

3. Security Affairs -- U.S. CISA adds iCagenda and Balbooa Forms flaws to its Known Exploited Vulnerabilities catalog (10 July 2026) -- <https://securityaffairs.com/195164/security/u-s-cisa-adds-icagenda-and-balbooa-forms-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

4. Security Affairs -- Adobe ColdFusion flaw CVE-2026-48282 now exploited in the wild (5 July 2026) -- <https://securityaffairs.com/194837/hacking/adobe-coldfusion-flaw-cve-2026-48282-now-exploited-in-the-wild.html>

5. Senserva -- CISA KEV Additions (July 2026): Vulnerabilities Exploited This Week (checked 12 July 2026) -- <https://serva.com/exploited-this-week.html>

6. Security Affairs -- Critical Gitea Docker bug under active exploitation exposes repositories and secrets (6 July 2026) -- <https://securityaffairs.com/194902/hacking/critical-gitea-docker-bug-under-active-exploitation-exposes-repositories-and-secrets.html>

11. IOL Business Report -- South Africa's data breaches could be costing the economy R142 billion a year (7 July 2026) -- <https://iol.co.za/business-report/economy/2026-07-07-south-africas-data-breaches-could-be-costing-the-economy-r142-billion-a-year/>

12. TechFinancials -- South Africa's costly data breaches: 1.81% GDP loss and the avoidable own-goals costing the economy (6 July 2026) -- <https://techfinancials.co.za/2026/07/06/south-africas-costly-data-breaches-1-81-gdp-loss-and-the-avoidable-own-goals-costing-the-economy/>

13. Sowetan -- Rise in data breaches puts influencers and everyday users at risk (8 July 2026) -- <https://www.sowetan.co.za/news/2026-07-08-rise-in-data-breaches-puts-influencers-and-everyday-users-at-risk/>

14. Engineering News -- POPIA five years later: why is nobody being held accountable? (6 July 2026) -- <https://www.engineeringnews.co.za/article/popia-five-years-later-why-is-nobody-being-held-accountable-2026-07-06>

15. ITWeb -- InfoReg exposes POPIA violators as data breaches mount (14 November 2025) -- <https://www.itweb.co.za/article/infoereg-exposes-popia-violators-as-data-breaches-mount/kLgB17ezby5M59N4>

16. Information Regulator (South Africa) -- Media statements (checked 12 July 2026; most recent statement dated 2 June 2026) -- <https://infoeregulator.org.za/media-statements/>

17. TechFinancials -- ICASA imposes multiple sanctions on SA telecoms provider (9 July 2026) -- <https://techfinancials.co.za/2026/07/09/icasa-imposes-multiple-sanctions-on-sa-telecoms-provider/>

18. TechFinancials -- Session Telecoms slaps regulator with legal challenge, alleges industry-wide fraud cover-up in R6m penalty row (9 July 2026) -- <https://techfinancials.co.za/2026/07/09/session-telecoms-slaps-regulator-with-legal-challenge-alleges-industry-wide-fraud-cover-up-in-r6m-penalty-row/>

20. ransomware.live -- South Africa victim map (checked 12 July 2026; 109 cumulative SA victims) -- <https://www.ransomware.live/map/ZA>

21. Data Breaches Digest -- Week 28 2026 edition, covering 6 - 12 July 2026 (checked 12 July 2026) -- <https://www.dbdigest.com/2026/07/data-breaches-digest-week-28-2026.html>

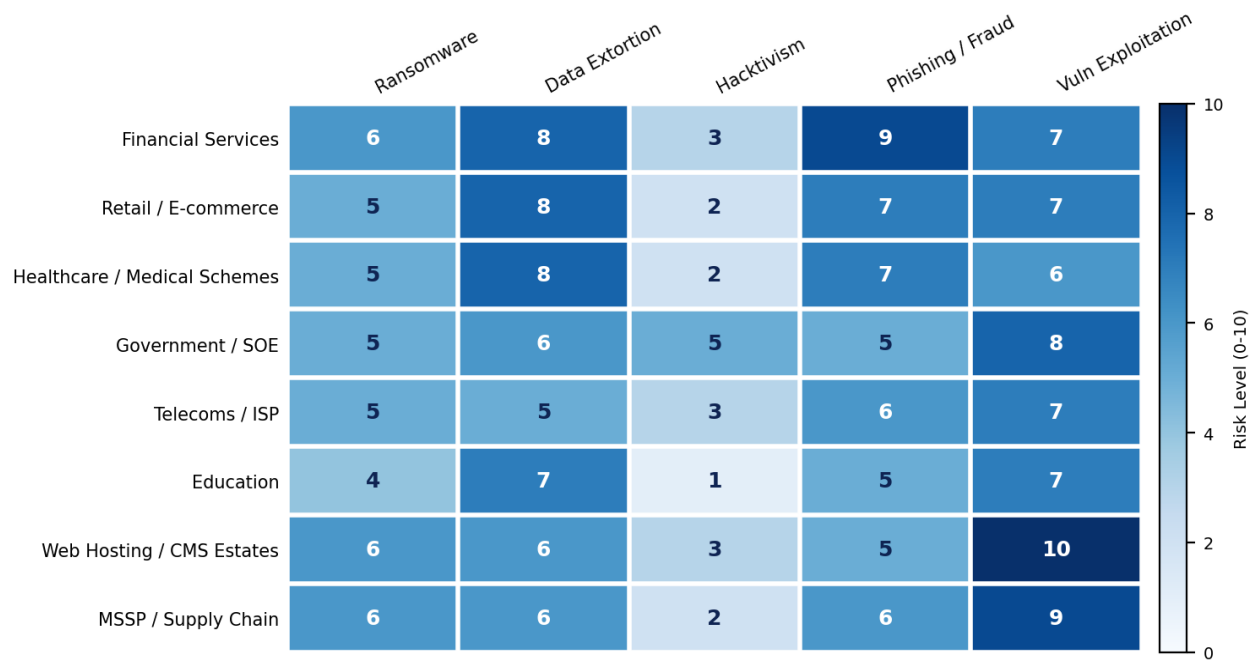
22. Breachsense -- Data breaches, July 2026 (checked 12 July 2026) -- <https://www.breachsense.com/breaches/2026/july/>

24. BleepingComputer -- Police arrest 5,800 suspects in global anti-fraud crackdown (9 July 2026) -- <https://www.bleepingcomputer.com/news/security/police-arrests-5-800-suspects-in-global-anti-fraud-crackdown/>

25. INTERPOL -- Over 5,800 arrests, USD 293 million intercepted in global fraud bust (July 2026) -- <https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W29 (5 July - 12 July 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting period, (b) active threat actor campaigns targeting the sector, (c) vulnerability exposure, and (d) regulatory scrutiny. **Critical (9-10)** = active exploitation or confirmed breach; **High (7-8)** = credible active threat; **Medium (4-6)** = elevated baseline risk; **Low (1-3)** = standard risk posture.

The single 10 this week sits on **Web Hosting / CMS Estates** for Vulnerability Exploitation: four of the six new KEV entries are Joomla third-party extension file-upload flaws under active mass exploitation, and the shared-hosting estates that run South African SME, NGO and municipal websites are the direct target surface.¹³ **MSSP / Supply Chain** holds 9 (ColdFusion, Gitea repository and CI-secret exposure, and the residual SimpleHelp RMM token problem).⁴⁶ **Government / SOE** rises to 8 on Vulnerability Exploitation on the same CMS logic -- municipal and departmental sites are disproportionately Joomla and WordPress -- while its Hacktivism score eases to 5: #OpSouthAfrica produced no observable activity in the window but has not been renounced. **Financial Services** retains 9 on Phishing / Fraud (tax season is open, and the ICASA SIM-boxing findings confirm that voice-channel manipulation infrastructure is operating inside SA networks).¹⁷ **Healthcare / Medical Schemes** and **Retail / E-commerce** ease from 9 to 8 on Data Extortion: the Profmed / PPSHA and Pick n Pay datasets remain in circulation, but neither saw a development this week.

3. TOP SA INCIDENTS (W29)

Week 29 (5 July - 12 July 2026) produced no new confirmed South African intrusion, breach disclosure or leak-site listing. The ransomware.live South Africa tally is unchanged at 109 (verified 12 July),²⁰ the Data Breaches Digest edition covering the window contains no SA victim,²¹ Breachsense lists none,²² and the ITWeb, TechCentral and IOL security desks published no SA incident story dated in the window.²⁷²⁸²⁹ The items below are therefore the week's material SA-relevant developments rather than fresh compromises. Each carries a confidence rating: CONFIRMED (victim/regulator acknowledgment or two independent sources), PROBABLE (single credible source), CLAIMED (threat-actor assertion only).

27. ITWeb -- Security section index (checked 12 July 2026; no SA incident reporting dated 5 - 12 July 2026) -- <https://www.itweb.co.za/categories/pXnWJadMba7bjO1e>

28. TechCentral -- News index (checked 12 July 2026; no SA incident reporting dated 5 - 12 July 2026) -- <https://techcentral.co.za/category/news/>

29. IOL -- Cyber attack tag index (checked 12 July 2026; most recent tagged item dated 15 June 2026) -- <https://iol.co.za/tags/cyber-attack/>

3.1 INC-2026-W29-01 -- Joomla-Ecosystem Mass Exploitation Wave Hits the SA SME and Municipal Web Stack [CONFIRMED]

Sector	Web hosting / CMS estates; SME, NGO, municipal and departmental websites
Date	Page Builder CK exploitation from 27 June 2026; KEV additions 7 July and 10 July 2026
Vulnerabilities	CVE-2026-48908 (JoomShaper SP Page Builder, CVSS 10.0, zero-day); CVE-2026-56290 (Joomlack Page Builder CK, 10.0); CVE-2026-48939 (iCagenda, 9.8); CVE-2026-56291 (Balbooa Forms, 9.8)
Mechanism	Unauthenticated or trivially authenticated arbitrary file upload leading to PHP execution; web shell drop; creation of new Joomla Super User accounts for persistence
Known artefacts	POST to index.php?option=com_sppagebuilder&task=asset.uploadCustomIcon; web shell at /media/com_pagebuilderck/gfonts/bhup.php keyed on the _upl POST parameter

SA relevance	No named SA victim. Joomla and its page-builder extensions are heavily represented in SA SME, NGO and local-government web estates, which are typically outsourced, unmonitored and unpatched
Confidence	CONFIRMED (campaign, CVEs, KEV listing and artefacts); no SA victim identified -- SA exposure is an inference from stack prevalence, not an observed compromise

Four of the six vulnerabilities CISA added to the KEV catalogue this week are file-upload flaws in third-party Joomla extensions, and the pattern is coordinated rather than coincidental: Page Builder CK exploitation began on 27 June within hours of the fix shipping, and SP Page Builder was exploited as a zero-day before any patch existed.¹²³ The attack chain is uniform -- upload a PHP file through a component that fails to validate type, execute it, then create a Super User account so the shell is redundant. This matters in South Africa not because a local victim has been named but because the exposed asset class is the one organisations do not think of as an asset: the brochure website, the events page, the contact form. Those sites frequently share hosting with, or hold credentials into, systems that do matter. Any organisation with a Joomla property should treat this as an active-exploitation event, patch to SP Page Builder 6.6.2+ and Page Builder CK 3.6.0, and hunt before assuming a clean bill of health.

3.2 INC-2026-W29-02 -- SA Breach Volume and Cost Made Public: 3,219 Notifications, R141.96bn, 1.81% of GDP [CONFIRMED as published; PROBABLE attribution]

Sector	Cross-sector / national economic exposure
Date	Published 6 July (TechFinancials) and 7 July 2026 (IOL Business Report)
Headline figures	3,219 breaches reported to the Information Regulator in FY2025/26; approximately 268 per month; estimated economic cost R141.96 billion; 1.81% of a R7.86 trillion GDP
Basis	Cube ICT Solutions analysis applying the IBM Cost of a Data Breach Report 2025 South African average of R44.1 million per breach to the reported breach count
Regulator's own last figures	2,374 notifications in FY2024/25 (about 198/month); 1,947 between April and November 2025 (about 284/month), a 40% year-on-year increase
Confidence	CONFIRMED (the figures as published, in two independent outlets); PROBABLE (the 3,219 total is a vendor analysis; no Information Regulator publication carrying that figure could be retrieved)

Two independent SA outlets carried the same analysis in the window: 3,219 breaches notified to the Information Regulator in the 2025/26 financial year, an estimated R141.96 billion of economic cost, and 1.81% of GDP.¹¹¹² The arithmetic is a simple multiplication of the reported breach count by the IBM South African average breach cost of R44.1 million, so it should be read as an order-of-magnitude indicator rather than a measured loss -- but the direction is unambiguous when set against the Regulator's own published series of 2,374 for FY2024/25 and a 40% year-on-year rise through late 2025.¹⁵ The operative number for boards is R44.1 million: the average South African breach now costs more than four times POPIA's R10 million maximum administrative fine, which means the regulatory penalty has stopped being the dominant financial risk in a breach.¹³¹⁴ Practitioner commentary published on 6 July frames the same data as an accountability gap: five years into POPIA, enforcement remains rare relative to incident volume.¹⁴

3.3 INC-2026-W29-03 -- ICASA Imposes R6m Penalty on Session Telecoms for SIM-Boxing and CLI Manipulation [CONFIRMED]

Sector	Telecommunications / Interconnect fraud
Date	ICASA Council approved the Complaints and Compliance Committee findings 18 June 2026; reported 9 July 2026
Origin	MTN complaint (April 2023) alleging CLI manipulation, call refiling and SIM-boxing; CCC hearings ran September 2023 to October 2025
Sanction	R3m under Regulation 6(3)(f) (use of invalid or unallocated numbers) plus R3m under Regulation 6(3)(g) (inefficient use of numbering resources); cease-and-desist; barring and withdrawal of numbering resources; monthly compliance reports including call records and international traffic for 24 months
Status	Session Telecoms has launched a legal challenge and alleges an industry-wide fraud cover-up
Confidence	CONFIRMED (regulator finding, reported with sanction detail); the operator's cover-up allegation is CLAIMED and untested

ICASA's finding is the week's only concrete South African enforcement action, and it is genuinely security-relevant rather than merely administrative: SIM-boxing and CLI manipulation are the infrastructure of interconnect-bypass fraud and, critically, of caller-ID spoofing used in vishing against bank customers.¹⁷ The regulator explicitly framed the sanction around the integrity and security of the national numbering system. The 24-month monthly reporting obligation, covering call records and international traffic, is the substantive remedy. Session Telecoms has taken the R6m penalty on review and alleges the practice is industry-wide; that allegation is untested.¹⁸ For banks and contact centres the operational read is unchanged: caller ID cannot be treated as an authentication factor.

3.4 INC-2026-W29-04 -- INTERPOL Operation First Light 2026: 5,811 Arrests, USD 293m Intercepted [CONFIRMED]

Sector	Global fraud enforcement (BEC, romance, investment, sextortion, impersonation)
Date	Operation ran 15 January - 30 April 2026; announced 9 July 2026
Results	5,811 arrests across 97 countries; USD 293 million intercepted; 142,000 victims identified; 31,014 accounts blocked; 15,606 further suspects identified
SA relevance	No SA-specific arrest figures published in the coverage retrieved; follows INTERPOL's Africa-focused Serengeti, Africa Cyber Surge and Red Card operations
Confidence	CONFIRMED (INTERPOL release plus independent reporting)

INTERPOL announced the results of Operation First Light 2026 on 9 July: 5,811 arrests across 97 countries and USD 293 million intercepted, targeting business email compromise, romance and investment scams, sextortion and impersonation fraud.²⁴²⁵ South African participation and any SA arrest numbers were not broken out in the coverage retrieved. The relevance for SA organisations is the account-blocking figure -- 31,014 accounts -- which indicates that mule-account networks, the mechanism through which SA-originated BEC and vishing losses are laundered, remain the enforcement pressure point.

Carryover Status (checked, no development 5 – 12 July 2026)

Pick n Pay Asap!/Bottles breach and Capitec card replacements: no development in the window; no further bank or retailer statements, and the dataset has not resurfaced in the aggregators checked.²¹²²

Profmed / PPS Healthcare Administrators: no scope expansion. The other four PPSHA-administered schemes -- KeyHealth, SEDMED, De Beers Benefit Society and the SANDF Regular Force Medical Continuation Fund -- have neither been confirmed nor excluded, and no Information Regulator statement has followed. This remains the highest-value unresolved SA exposure. **Standard Bank / Liberty (Prinz Eugen / ROOTBOY):** no new public development; the ransomware.live listing is unchanged.²⁰ **AVBOB Mutual Assurance:** approximately six weeks post-incident, still no leak-site claim or attribution -- the exposure remains UNDETERMINED. **#OpSouthAfrica (Nullsec Nigeria / Anonymous Nigeria):** no new leaks, defacements or claims in the window. Exfiltrated Department of Correctional Services data remains in actor hands and the campaign has not been renounced; treat as dormant, not resolved. Caveat: Telegram and dark-web channels were not directly observable. **SAPS Western Cape POPIA breach (3,000 officers' medical records):** no Information Regulator statement or investigation outcome; the Regulator's media-statements page, checked 12 July, shows nothing newer than 2 June.¹⁶ **Tembisa Hospital information-officer prosecution:** no prosecution decision published following the lapsed hand-over window.

Verification Note -- Western Cape Provincial Legislature

A Sowetan article published 8 July 2026 carries social-preview image metadata reading 'Services are being restored after a cybersecurity breach at the provincial legislature in the Western Cape.'¹³ This is recycled content-management metadata attached to a stock photograph; the article body concerns breach statistics and makes no reference to the Western Cape Provincial Parliament. No primary reporting of a 2026 WCPP breach exists in any source checked. The caption is an artefact of the 2023 WCPP incident and should not be treated as a current event. It is recorded here because the metadata is machine-readable and will otherwise propagate into automated feeds.

4. THREAT ACTORS

4.1 Joomla-Extension Exploitation Cluster [CONFIRMED campaign; UNATTRIBUTED]

An unattributed but evidently coordinated cluster is systematically weaponising file-upload flaws across unrelated Joomla third-party extensions -- SP Page Builder, Page Builder CK, iCagenda and Balbooa Forms -- with all four reaching the KEV catalogue within four days of each other.¹³ Tradecraft is consistent: unauthenticated PHP upload, web shell, then Super User account creation for persistence that survives shell removal. The reporting chain runs through the Joomla monitoring vendor mySites.guru. The timing -- Page Builder CK exploited within hours of its fix, SP Page Builder exploited before one existed -- indicates the operator is monitoring extension release channels rather than scanning opportunistically. Highest-priority actor for SA web estates this week.

4.2 Adobe ColdFusion RDS Exploiters [PROBABLE]

Exploitation of CVE-2026-48282 began within two hours of public disclosure, with the first observed attempt attributed in vulnerability-intelligence reporting to 103.207.14[.]220 (India-geolocated).¹⁴ No actor name, no ransomware linkage established. The sub-two-hour turnaround is the point: for maximum-severity, unauthenticated, internet-reachable flaws, the window between disclosure and exploitation is now shorter than most change-approval cycles. Single-IP attribution should be treated as an early indicator, not a complete infrastructure picture.

4.3 Langflow / AI-Platform Operator [CONFIRMED research]

Sysdig research documents a single operator at 45.207.216[.]155 chaining Langflow CVE-2026-55255 (authorization bypass through a user-controlled key, cross-tenant IDOR) with CVE-2026-33017 (RCE) between 22 and 25 June, stealing LLM-provider API keys and AWS credentials in behaviour consistent with cryptojacking and botnet monetisation.¹⁵ This is the first AI-agent orchestration platform to reach the KEV catalogue in this cycle and it establishes the pattern SA organisations should expect: AI tooling is being attacked not for its models but for the cloud and provider credentials it holds.

4.4 Qilin, Safepay and Braincipher [CONFIRMED postings; info-stealer precursor]

The active leak-site posters in the window were Qilin (Cash Canada, 24 June; Chamco, 30 June), Safepay (rtngmbh.de, 6 July) and Braincipher (themintgaming.com, 19 June); no South African victims.²³ The common thread across the victims is prior credential theft by Cavalier-family info-stealers rather than a shared CVE -- the ransomware event is the last step of an info-stealer chain that began weeks earlier. This is the single most transferable lesson for SA mid-market defenders: the intervention point is the stolen credential, not the encryption.

4.5 Prinz Eugen / ROOTBOY [CONFIRMED profile; no in-window development]

Go-based data-extortion operator (ChaCha20-Poly1305 with Argon2id/HKDF derivation, no ransom note on disk, RemotePC RMM persistence, stolen-RDP initial access) behind the Standard Bank / Liberty leak. No new public development in the window; the ransomware.live listing is unchanged.²⁰ Claims of escalating daily Standard Bank data dumps remain CLAIMED and uncorroborated.

4.6 Nullsec Nigeria / Anonymous Nigeria (#OpSouthAfrica) [CONFIRMED campaign; dormant]

No observable activity in the window -- a second consecutive quiet week following the 30 June flashpoint that passed without escalation. Exfiltrated Department of Correctional Services data remains unreleased and the campaign has not been renounced. Government and SOE defenders should treat the reduced tempo as an opportunity to remediate the known exposed municipal and justice-system estate, not as a reason to stand down.

4.7 Law-Enforcement Attrition: Ryuk and the Fraud Ecosystem [CONFIRMED]

INTERPOL's Operation First Light 2026 produced 5,811 arrests and USD 293 million intercepted across 97 countries,^{24,25} and Armenian national Karen Serobovich Vardanyan pleaded guilty in the United States on 10 July to Ryuk ransomware involvement covering roughly 1,610 BTC (about USD 15 million) in ransoms, with sentencing set for September 2026.²⁶

23. Quasar CyberTech Q-Pulse -- Multiple ransomware groups target diverse organizations in June and July 2026 (6 July 2026) -- <https://qpulse.quasarcybertech.com/news/4219/multiple-ransomware-groups-target-diverse-organizations-in-june-and-july-2026>

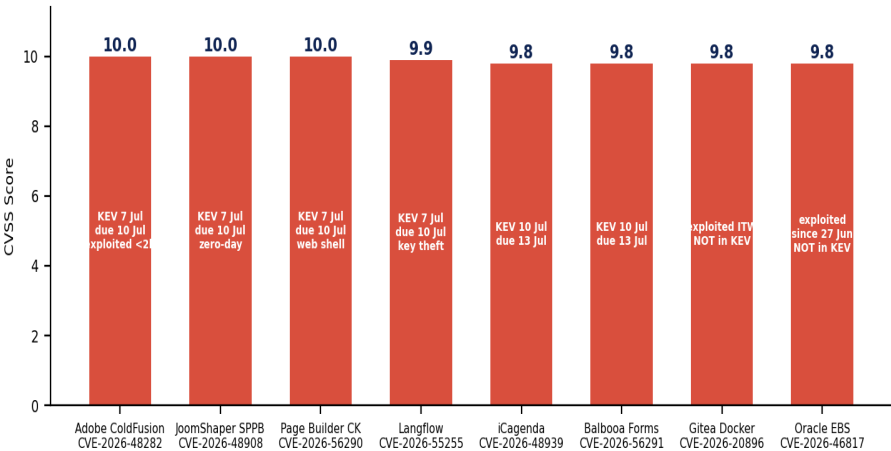
26. BleepingComputer -- Ryuk ransomware member pleads guilty in the US, faces 15 years in prison (10 July 2026) -- <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-member-pleads-guilty-in-the-us-faces-15-years-in-prison/>

5. CRITICAL VULNERABILITIES & CISA KEV

Six vulnerabilities entered the CISA KEV catalogue between 5 and 12 July 2026 -- four on 7 July and two on 10 July -- and every one of them is rated CVSS 9.8 or higher.¹³⁵ Two structural observations matter more than the individual CVEs. First, the remediation clock: the required-action text on these entries cites BOD 26-04 rather than BOD 22-01, giving federal agencies roughly three days rather than three weeks. The 7 July batch was due 10 July; the 10 July batch is due 13 July. Short fuses are no longer the exception -- they are the standing regime, and any SA patch process built around a 21-day KEV assumption is now calibrated to the wrong number. Second, the composition: four of the six are third-party Joomla extension file-upload flaws, which means the KEV catalogue this week is not describing enterprise infrastructure at all. It is describing websites. Note that CISA KEV facts in this report are anchored to multiple independent fetched secondary sources quoting the CISA alerts, because cisa.gov blocks direct automated retrieval from our fetch environment.

W29 KEV / Critical CVE Severity Overview -- (6 New KEV Adds 5 - 12 Jul + Exploited-but-Unlisted)

W29 KEV / CRITICAL CVE SEVERITY | 5 July - 12 July 2026
6 new KEV entries, all CVSS 9.8-10.0, all on a 3-day BOD 26-04 remediation clock; 4 of 6 are Joomla third-party extension file-upload flaws; Gitea and Oracle EBS exploited without a KEV listing



W29 CISA KEV / Critical CVE Tracking (new adds 5 - 12 July + active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-48282	Adobe ColdFusion (2025.9, 2023.20 and earlier; RDS FILEIO handler)	10.0	Path traversal to unauth RCE	10 Jul 2026 (LAPSED)	KEV 7 Jul; exploited under 2 hours after disclosure; first attempt from 103.207.14[.]220; patched 30 Jun alongside five other maximum-severity ColdFusion bugs; disable RDS in production

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-48908	JoomShaper SP Page Builder (Joomla)	10.0	Unrestricted file upload to RCE	10 Jul 2026 (LAPSED)	KEV 7 Jul; exploited as a ZERO-DAY; POST to asset.uploadCustomIcon then Super User creation; fix SP Page Builder 6.6.2+
CVE-2026-56290	Joomla Page Builder CK (Joomla)	10.0	Improper access control to file upload	10 Jul 2026 (LAPSED)	KEV 7 Jul; exploited from 27 Jun, hours after the fix shipped; web shell /media/com_pagebuilderck/gfonts/bhup.php keyed on _upl; fix Page Builder CK 3.6.0
CVE-2026-55255	Langflow (DataStax)	9.9	Authz bypass (user-controlled key)	10 Jul 2026 (LAPSED)	KEV 7 Jul; cross-tenant IDOR chained with CVE-2026-33017 RCE 22-25 Jun from 45.207.216[.]55; LLM and AWS key theft. Note: one outlet prints CVSS 6.1; KEV/NVD-derived trackers and Sysdig give 9.9
CVE-2026-48939	iCagenda (Joomla event extension)	9.8	Unrestricted file upload	13 Jul 2026	KEV 10 Jul; attachment feature permits PHP upload and execution; deadline falls the day the SA business week opens
CVE-2026-56291	Balbooa Forms (Joomla)	9.8	Unauth arbitrary file upload	13 Jul 2026	KEV 10 Jul; unauthenticated upload of executable files leading to full RCE
CVE-2026-20896	Gitea (official Docker images <= 1.26.2)	9.8	Reverse-proxy auth bypass	NOT IN KEV (12 Jul)	Exploited ITW; images ship REVERSE_PROXY_TRUSTED_PROXYIES as a wildcard; X-WEBAUTH-USER header authenticates as any user; ~6,200 exposed instances; fix 1.26.3 / 1.26.4 and rotate CI secrets
CVE-2026-46817	Oracle EBS Payments (12.2.3-12.2.15)	9.8	Unauth file read	NOT IN KEV (12 Jul)	CARRYOVER: exploited ITW since 27 Jun (day 15); ~950 exposed instances; /OA_HTML/ibytransmit; still unlisted after two weeks -- do not wait for the catalogue
CVE-2026-50746	Ubiquiti UniFi Connect Application (<= 3.4.16)	10.0	Command injection	n/a (patched 8 Jul)	One of seven UniFi flaws disclosed 8 Jul (bulletin 066); no confirmed ITW exploitation; separate from the 23 Jun UniFi OS KEV trio

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-48558	SimpleHelp RMM	n/r	Auth bypass (OIDC)	7 Jul 2026 (LAPSED)	CARRYOVER: no post-deadline exploitation reporting surfaced 5-12 Jul. Stolen tokens survive patching -- rotate credentials issued through SimpleHelp-managed environments
CVE-2026-45659	Microsoft SharePoint Server (SE, 2019, 2016)	8.8	Deserialization RCE	4 Jul 2026 (LAPSED)	CARRYOVER: no new exploitation reporting in the window; apply the May 2026 fix if the deadline was missed

Pattern note: W29 inverts the usual shape of a KEV week. The volume tripled (six adds versus two), the severity floor rose to 9.8, and the fuse shortened to roughly three days -- but the target class moved down-market, from enterprise infrastructure to website plugins. Four Joomla extension flaws in a single week means the exploitation frontier has moved to assets that most organisations do not inventory, do not monitor and cannot name an owner for. At the same time, two of the week's most dangerous flaws (Gitea 9.8 and Oracle EBS 9.8) are being exploited without any KEV listing at all. The operating lesson is the same in both directions: the KEV catalogue is a floor for prioritisation, not the boundary of the problem.

Patch Tuesday and Corrections

Patch Tuesday, 14 July 2026: the July release lands the day after publication. Ivanti's forecast, published 10 July, expects continued elevated CVE volume after June's 206 CVEs and three zero-days, with SQL Server possibly in rotation.⁹ A Microsoft Defender race-condition privilege escalation (CVE-2026-50656, publicly named 'RoguePlanet', with a proof-of-concept yielding a SYSTEM shell) was fixed out of band on 9 July and is therefore unlikely to feature as an open Patch Tuesday zero-day. Adobe has moved to two security releases per month; the Oracle Critical Patch Update follows on 21 July. **Correction to DP-CTI-2026-W28:** that edition listed the Ubiquiti UniFi OS trio (CVE-2026-34908/-09/-10) and Lantronix EDS5000 (CVE-2025-67038) as carrying KEV due dates of 14 July 2026. On re-verification those entries were added to the KEV catalogue on 23 June under the BOD 26-04 three-day clock, with remediation due 26 June -- they are OVERDUE, not upcoming.¹⁰ Organisations that scheduled them against a 14 July date should re-prioritise immediately. Equally, the KB5094126 Recycle Bin fix and the BitLocker lockout acknowledgment carried as W29 watch items could not be verified in any fetchable source this week; the only corroborated Windows Server 2025 known issue is the Recycle Bin displaying internal file names. Those items are withdrawn pending confirmation. **Ubiquiti:** a separate advisory on 8 July (bulletin 066) disclosed seven UniFi flaws, led by CVE-2026-50746 (CVSS 10.0, command injection in UniFi Connect Application 3.4.16 and earlier); there is no confirmed in-the-wild exploitation, but SA estates running UniFi Connect for building systems should patch on the standard cycle.⁷ **Zimbra:** ZCS 10.1.19, released 10 July, fixes a critical stored cross-site scripting flaw in the Classic Web Client that executes on message open; no CVE has been assigned and there is no evidence of exploitation, but SA organisations running on-premises Zimbra should patch on the standard cycle.⁸

7. Security Affairs -- Ubiquiti patches critical UniFi OS flaws allowing command injection and privilege escalation (8 July 2026) -- <https://securityaffairs.com/194978/security/ubiquiti-patches-critical-unifi-os-flaws-allowing-command-injection-and-privilege-escalation.html>

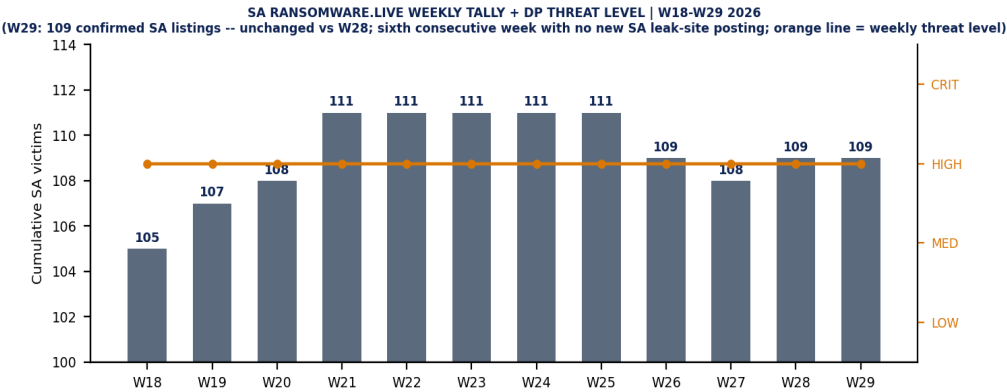
8. Security Affairs -- Update now: critical Zimbra Classic Web Client flaw could expose mailboxes (10 July 2026) -- <https://securityaffairs.com/195130/hacking/update-now-critical-zimbra-classic-web-client-flaw-could-expose-mailboxes.html>

9. Help Net Security -- July 2026 Patch Tuesday forecast (10 July 2026) -- <https://www.helpnetsecurity.com/2026/07/10/july-2026-patch-tuesday-forecast/>

10. Security Affairs -- U.S. CISA adds Ubiquiti UniFi OS and Lantronix EDS5000 plugin flaws to its Known Exploited Vulnerabilities catalog (23 June 2026) -- <https://securityaffairs.com/194142/security/u-s-cisa-adds-ubiquiti-unifi-os-and-lantronix-eds5000-plugin-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

6. RANSOMWARE LANDSCAPE

The ransomware.live cumulative South Africa count is 109, verified 12 July via the country map.²⁰ That is unchanged from W28's 109: no new SA victim was posted, and no listing was removed. The most recent discovery date anywhere in the ZA dataset remains 2 June 2026 (African National Congress -- Black X), followed by 4 May (Standard Bank Group -- Prinz Eugen) and 3 May (Consumer Goods Council of SA -- Stormous). This is now the sixth consecutive week without a confirmed new South African leak-site posting. That streak deserves a caution rather than a celebration. Leak-site absence measures publication, not compromise: a victim that pays quietly, an actor that has not yet finished negotiating, and a group that never posts all look identical from the outside. The SA breach series -- 3,219 notifications to the Information Regulator in FY2025/26, roughly 268 a month -- describes an incident rate two orders of magnitude above what leak sites show.¹¹ The leak-site count is a floor on SA ransomware activity, not a measurement of it.



End W28 baseline	109 confirmed SA listings
New W29 listings (5 - 12 Jul)	0 confirmed on ransomware.live; 0 SA items in Data Breaches Digest week 28; 0 SA entries in Breachsense July list
Delistings / restorations (W29)	0 observed
End W29 count	109 (no change vs W28; verified 12 July via country map)
Most recent SA discovery dates	2 Jun (ANC -- Black X); 4 May (Standard Bank Group -- Prinz Eugen); 3 May (CGCSA -- Stormous)
Quiet streak	6 consecutive weeks with no new confirmed SA leak-site posting

Threat-level drivers (non-ransomware.live)	Joomla-ecosystem mass exploitation reaching SA SME and municipal web estates; Adobe ColdFusion CVSS 10.0 exploited within 2 hours; Gitea and Oracle EBS exploited without KEV listing; SA breach cost disclosure; Information Regulator silence
--	---

Group notes: **Qilin** posted Cash Canada (24 June) and Chamco (30 June); **Safepay** posted rtngmbh.de (6 July); **Braincipher** posted themintgaming.com (19 June) -- no SA victims among them, and the shared precursor across the set is Cavalier-family infostealer credential theft rather than a common exploited CVE.²³ **Prinz Eugen** -- no leak-site movement (Section 4.5). **The Gentlemen / GentleKiller, DragonForce, KillSec, BlackSuit, Nightspire, Interlock, XP95 and Stormous** -- checked, no in-window SA or Africa developments. **Law enforcement:** INTERPOL Operation First Light 2026 (5,811 arrests, USD 293m intercepted, announced 9 July) is the window's principal action, alongside the Ryuk guilty plea of 10 July.²⁴²⁵²⁶ **Africa reporting:** no new Africa-specific vendor or law-enforcement threat assessment was published in the window; the INTERPOL Africa Cyberthreat Assessment 2025 (17,849 ransomware detections in South Africa in 2024, the continental high) remains the standing reference.

7. OSINT EXPOSURE & ATTACK SURFACE

The unmanaged CMS estate -- this week's dominant SA exposure

The Joomla wave makes an uncomfortable point about attack-surface management: most South African organisations can produce a server inventory but not a website inventory. Marketing microsites, event registration pages, NGO partner portals, municipal notice boards and legacy campaign sites are typically built by an agency, handed over, and never patched again. Four unauthenticated file-upload RCEs in commonly installed Joomla extensions -- SP Page Builder, Page Builder CK, iCagenda and Balbooa Forms -- turn that inventory gap directly into remote code execution on shared hosting that often sits one credential away from something that matters.¹³ The practical exercise this week is dull and high-yield: pull the DNS zone, enumerate every hostname that resolves, fingerprint the CMS, and assign an owner to each. Anything unowned should be taken offline rather than patched.

Gitea -- source code and CI secrets reachable from a single HTTP header

Roughly 6,200 Gitea instances are internet-exposed, and official Docker images at or below 1.26.2 ship with REVERSE_PROXY_TRUSTED_PROXIES set to a wildcard. Where reverse-proxy authentication is enabled, any source IP can supply an X-WEBAUTH-USER header naming any valid user -- including an administrator -- and be authenticated. Exploitation in the wild was observed thirteen days after the advisory. SA development shops and MSPs self-hosting Gitea should upgrade to 1.26.3 or 1.26.4, explicitly restrict trusted proxies, and treat repository secrets, deploy keys and CI tokens as exposed until rotated.⁶

Oracle E-Business Suite -- exploited, exposed and still unlisted

Shadowserver's count of roughly 950 internet-exposed Oracle EBS instances is unchanged, and CVE-2026-46817 (CVSS 9.8, unauthenticated file read reaching database credentials and payment API keys via /OA_HTML/ibytransmit) has now been exploited in the wild for over two weeks without a KEV listing. SA organisations running EBS should establish their exposure and sweep for POSTs to /OA_HTML/ibytransmit dating from 27 June, irrespective of the catalogue.

Standing SA government web-estate baseline (pre-window)

GroundUp's June investigation remains the freshest public SA attack-surface dataset: 1,089 exposed service records across 516 non-SITA .gov.za hosts, 106 of them (about one in five) vulnerable, with 4,466 CVEs including 726 critical. Read alongside the Joomla wave, that baseline is the most likely path to a South African victim in the coming weeks: an unpatched municipal CMS is both the easiest target on the list and the one least likely to have a defender assigned to it.

8. REGULATORY & POLICY

Information Regulator -- a sixth week of public silence [CONFIRMED]

The Regulator's media-statements page, checked 12 July, carries nothing dated after 2 June 2026.¹⁶ No enforcement notice, infringement notice, guidance note or statement was published in the window. That silence is itself the regulatory story of the week, because it sits directly alongside the publication of the breach-volume figures: 3,219 notifications in FY2025/26 against a Regulator that has issued a handful of infringement notices, several of which remain unpaid and are being pursued through the courts (Blouberg Municipality R500,000, FT Rams R100,000).¹¹¹⁵ Practitioner commentary published 6 July puts the position bluntly: five years into POPIA, compliance documentation is abundant and accountability is not.¹⁴

TransUnion SA / Experian SA: the section 59 notices reported in W27 required responses by approximately 6 July. That date has passed with no statement from the Regulator, no statement from either bureau, and no coverage -- a second consecutive week of silence on the highest-profile open POPIA matter. Organisations consuming bureau data should not read the absence of news as a resolution. **Tembisa Hospital / Gauteng Health:** no prosecution decision published following the lapsed hand-over window.

ICASA -- R6m penalty for SIM-boxing and CLI manipulation [CONFIRMED]

ICASA's Council approved its Complaints and Compliance Committee findings against Session Telecoms on 18 June, reported 9 July: R3 million under Regulation 6(3)(f) and R3 million under Regulation 6(3)(g), cease-and-desist orders, barring and withdrawal of numbering resources, and 24 months of monthly compliance reporting covering call records and international traffic.¹⁷ The underlying MTN complaint alleged CLI manipulation, call refiling and SIM-boxing. This is the first substantive SA regulatory action in weeks and the first in some time to bite on the infrastructure of telecoms fraud rather than on data processing. Session Telecoms has launched a legal challenge and alleges the practice is industry-wide -- an untested CLAIMED assertion, but one worth tracking, because if borne out it would indicate that caller-ID spoofing capability is more widely available inside SA networks than currently assumed.¹⁸

FIC -- CCR live, no first-week enforcement visible [CONFIRMED go-live; nil enforcement]

The cross-border cash conveyance reporting regime commenced 1 July: travellers crossing any SA air, land or sea border with cash or bearer negotiable instruments above R100,000 must declare through the SARS Customs traveller management system, with the commencement proclamation of 5 June bringing FICA sections 30, 54, 55 and 70 into force -- wilful failure to report is a criminal offence and section 70 provides for search, seizure and mandatory forfeiture on conviction.¹⁹ No seizures, forfeitures or FIC operational statements had been published by 12 July. Closing the W28 watch item: no final 2026 Risk and Compliance Return first-batch filing tally has been published either. The second-batch deadline -- legal practitioners, estate agents, high-value goods dealers and non-casino gambling -- remains 31 July, and accountable institutions in that cohort should file rather than wait for FIC messaging.

What SA businesses should read into the week's numbers [ANALYSIS]

The R44.1 million average South African breach cost is now more than four times POPIA's R10 million maximum administrative fine.¹³ That inversion changes the compliance argument materially: for most organisations the regulator is no longer the expensive part of a breach. Boards that have been sizing security investment against the fine are sizing it against the wrong number by a factor of four, before counting customer churn, remediation and downtime. The corollary for the Regulator is uncomfortable and was made publicly this week: a penalty ceiling that sits below the average cost of the harm it is meant to deter is not a deterrent.¹⁴

19. Engineering News -- Domestic, foreign travellers must now declare cash of more than R100 000 -- FIC (1 July 2026) -- <https://www.engineeringnews.co.za/article/domestic-foreign-travellers-must-now-declare-cash-of-more-than-r100-000-fic-2026-07-01>

9. WEEKLY THREAT HUNT & IOCs

Eight hunt missions are active for W29, weighted to the week's dominant theme -- exploitation of internet-facing web and developer infrastructure. Three P1 missions cover the Joomla extension wave (four KEV entries, confirmed web-shell and persistence artefacts), Adobe ColdFusion CVE-2026-48282 (CVSS 10.0, exploited within two hours of disclosure) and the Langflow AI-platform credential-theft chain. Three P2 missions cover Gitea reverse-proxy authentication bypass, the still-unlisted Oracle EBS Payments exploitation, and residual SimpleHelp RMM token exposure. Two P3 missions address the infostealer-to-ransomware precursor chain and a South African CMS attack-surface sweep. A machine-readable indicator export accompanies this report (iocs_w29.csv).

TH-2026-W29-01 -- Joomla Extension File-Upload Web Shell Hunt

P1 -- CRITICAL: 4 KEV entries, CVSS 9.8-10.0; deadlines 10 Jul (lapsed) and 13 Jul

Hypothesis: An unauthenticated attacker uploads a PHP file through a vulnerable Joomla third-party extension (SP Page Builder CVE-2026-48908, Page Builder CK CVE-2026-56290, iCagenda CVE-2026-48939, Balbooa Forms CVE-2026-56291), executes it as a web shell, and creates a new Joomla Super User account so that access survives shell removal and patching.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Server Software Component: Web Shell), T1136.001 (Create Account: Local Account), T1078 (Valid Accounts).

IOCs: Web shell path /media/com_pagebuilderck/gfonts/bhup.php (keyed on the _upl POST parameter); POST requests to index.php?option=com_sppagebuilder&task=asset.uploadCustomIcon; any newly written .php file under /media/, /images/ or /tmp/ on a Joomla root; new rows in the #__users table with Super Users group membership; unexpected .phtml, .phar or double-extension uploads.

Data Sources: Web-server access logs (POST with multipart/form-data to component endpoints), WAF logs, file-integrity monitoring on the webroot, Joomla user-action logs, hosting-provider audit logs, EDR on the web tier.

Detection Guidance: Alert on any newly created executable file under a Joomla media or upload directory -- that directory should never contain PHP. Alert on Super User account creation outside a change window. Patch to SP Page Builder 6.6.2+ and Page Builder CK 3.6.0, update iCagenda and Balbooa Forms, and remove unused extensions entirely. After patching, still hunt: the persistence account survives the fix.

TH-2026-W29-02 -- Adobe ColdFusion CVE-2026-48282 RDS Path Traversal Hunt	P1 -- CRITICAL: CVSS 10.0; exploited <2h post-disclosure; KEV deadline 10 Jul LAPSED
Hypothesis: An unauthenticated attacker abuses the RDS FILEIO handler path traversal in ColdFusion 2025.9 / 2023.20 and earlier to write an arbitrary file to the webroot and achieve remote code execution. Any internet-facing unpatched instance between 30 June and 7 July should be assumed reachable. MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter), T1005 (Data from Local System). IOCs: Source IP 103.207.14[.]220 (first observed exploitation attempt); requests to RDS endpoints (/CFIDE/main/ide.cfm, RDS FILEIO paths) containing traversal sequences; newly written .cfm or .jsp files in the ColdFusion webroot; ColdFusion service spawning cmd.exe, powershell.exe or /bin/sh. Data Sources: ColdFusion access and application logs, IIS/Apache logs, EDR process-lineage telemetry on ColdFusion hosts, file-integrity monitoring on the webroot, egress netflow. Detection Guidance: Apply the 30 June Adobe update. Disable RDS in production -- it should never be enabled on an internet-reachable server. Block the RDS endpoints at the WAF. If the host was exposed and unpatched in the exploitation window, run a compromise assessment rather than relying on the patch: file write happened before the fix landed.	
TH-2026-W29-03 -- Langflow / AI-Platform Cross-Tenant IDOR and Secret Theft Hunt	P1 -- CRITICAL: CVSS 9.9; chained with RCE; LLM and cloud key theft
Hypothesis: An operator exploits Langflow CVE-2026-55255 (authorization bypass through a user-controlled key -- cross-tenant IDOR) chained with CVE-2026-33017 (RCE) to read other tenants' flows and steal the LLM-provider API keys and AWS credentials stored in them, monetising via cryptojacking or botnet resale. MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1552.001 (Unsecured Credentials: Credentials in Files), T1528 (Steal Application Access Token), T1496 (Resource Hijacking). IOCs: Source IP 45.207.216[.]55; Langflow API requests referencing flow or component identifiers outside the caller's tenant; anomalous outbound calls to LLM provider endpoints; sudden AWS API activity from new regions or new access-key IDs; new EC2 or container workloads with high CPU. Data Sources: Langflow application logs, reverse-proxy logs, AWS CloudTrail (GetCallerIdentity, RunInstances, CreateAccessKey), LLM-provider usage and billing telemetry, cloud cost anomaly alerts. Detection Guidance: Patch Langflow. Treat every API key and cloud credential stored in a Langflow flow as compromised and rotate it -- patching does not invalidate stolen keys. More broadly: inventory AI orchestration platforms as credential stores, because that is what attackers are treating them as. Put them behind SSO and network restrictions; they should not be internet-reachable.	

TH-2026-W29-04 -- Gitea Reverse-Proxy Authentication Bypass Hunt

P2 -- HIGH: CVSS 9.8; exploited ITW; NOT in KEV; ~6,200 exposed instances

Hypothesis: An unauthenticated attacker sends a crafted X-WEBAUTH-USER header to a self-hosted Gitea instance running an official Docker image at or below 1.26.2 (which ships REVERSE_PROXY_TRUSTED_PROXIES as a wildcard) and is authenticated as any named user, including an administrator, gaining access to private repositories, CI secrets and deploy keys.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078.001 (Valid Accounts: Default Accounts), T1552.007 (Container API), T1213.003 (Data from Information Repositories: Code Repositories).

IOCs: Inbound HTTP requests carrying an X-WEBAUTH-USER header from a source outside the reverse-proxy IP range; Gitea configuration with REVERSE_PROXY_TRUSTED_PROXIES = *; Gitea versions <= 1.26.2 on official Docker images; repository clone or archive-download bursts from a single IP; new personal access tokens or SSH keys on admin accounts.

Data Sources: Gitea access and admin-audit logs, reverse-proxy (nginx/Traefik) logs, container image inventory, egress netflow from the Git host, secret-scanning alerts on downstream CI.

Detection Guidance: Upgrade to Gitea 1.26.3 or 1.26.4. Explicitly set REVERSE_PROXY_TRUSTED_PROXIES to the proxy IPs only, and strip X-WEBAUTH-USER at the edge. Rotate all repository secrets, deploy keys and CI tokens if the instance was internet-facing on a vulnerable image.

TH-2026-W29-05 -- Oracle EBS Payments CVE-2026-46817 Exploitation Hunt (Day 15, Still Not in KEV)

P2 -- HIGH: CVSS 9.8; exploited since 27 Jun; ~950 exposed instances; unlisted

Hypothesis: An unauthenticated attacker reaches the Oracle E-Business Suite Payments / File Transmission endpoint on an internet-facing instance (EBS 12.2.3 to 12.2.15) and reads arbitrary files, obtaining database credentials and payment API keys. Exploitation has run for over two weeks without a KEV listing to trigger internal patch SLAs.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1005 (Data from Local System), T1552.001 (Unsecured Credentials), T1078 (Valid Accounts).

IOCs: POST requests to /OA_HTML/ibytransmit from 27 June 2026 onward; requests to /OA_HTML/ containing traversal or file-parameter manipulation; anomalous reads of context files and wallet/keystore paths; subsequent database logons from application-tier credentials at unusual hours.

Data Sources: Oracle EBS application and Apache logs, WAF logs, database audit logs (logon source and time), netflow from the EBS tier, external exposure scans.

Detection Guidance: Apply the relevant Oracle Critical Patch Update; the next CPU is 21 July. Remove EBS from direct internet exposure or place it behind a VPN or reverse proxy with authentication. Rotate database credentials and payment API keys if the instance was exposed and unpatched after 27 June. Do not wait for a KEV listing -- the catalogue has not caught up with this one.

TH-2026-W29-06 -- SimpleHelp RMM Residual Token Exposure Hunt (Post-Deadline Carryover)

P2 -- HIGH: KEV deadline 7 Jul LAPSED; stolen tokens survive patching

Hypothesis: An MSP or customer environment managed through SimpleHelp was accessed via CVE-2026-48558 (OIDC auth bypass) before patching, and the attacker retains valid cloud, source-control, package-registry, SSH and AI-assistant tokens harvested by the TaskWeaver loader and Djinn Stealer. Patching closed the door; it did not revoke the keys.

MITRE ATT&CK: T1219 (Remote Access Software), T1555 (Credentials from Password Stores), T1528 (Steal Application Access Token), T1199 (Trusted Relationship).

IOCs: SimpleHelp Technician sessions from unexpected source IPs or at unusual hours; TaskWeaver Node.js loader artefacts; Djinn Stealer execution; use of cloud, SCM or registry tokens from IPs never previously seen for that principal; SSH key use from new hosts.

Data Sources: SimpleHelp server session logs, EDR on RMM-managed endpoints, cloud IAM logs (token use by source IP), SCM audit logs (GitHub/GitLab/Bitbucket), package-registry publish logs, SSH auth logs.

Detection Guidance: Confirm the patch, then rotate every credential that was reachable from a SimpleHelp-managed host. MSP customers should require written attestation of both patching and rotation. Baseline token use by source IP and alert on first-seen combinations. No post-deadline exploitation reporting appeared in 5-12 July, which lowers urgency but does not close the exposure.

TH-2026-W29-07 -- Infostealer-to-Ransomware Precursor Hunt

P3 -- MEDIUM: shared precursor across Qilin, Safepay and Braincipher victims

Hypothesis: Ransomware deployment in the window's observed victims was preceded by Cavalier-family infostealer credential theft rather than a common exploited CVE. Corporate credentials harvested from an employee's personal or unmanaged device appear in a stealer log, are purchased, and are used for initial access weeks later. The detectable event is the credential, not the encryption.

MITRE ATT&CK: T1555.003 (Credentials from Web Browsers), T1078 (Valid Accounts), T1133 (External Remote Services), T1486 (Data Encrypted for Impact).

IOCs: Corporate email addresses or domains appearing in stealer-log dumps and combolists; VPN, VDI or M365 logons from residential-proxy or unusual-geography IPs using valid credentials without MFA; impossible-travel authentications; session-cookie replay without a preceding password event.

Data Sources: Identity provider sign-in logs (M365 / Entra ID, Okta), VPN concentrator logs, dark-web and stealer-log monitoring services, haveibeenpwned-style domain notifications, EDR on BYOD-adjacent assets.

Detection Guidance: Enforce phishing-resistant MFA on every external entry point -- this chain dies at MFA. Subscribe to stealer-log monitoring for your corporate domains and treat a hit as an incident, not a newsletter item. Force password and session-token reset on any exposed account. This is the single highest-yield control for SA mid-market organisations, which are far more likely to be ransomed via a stolen credential than via a zero-day.

TH-2026-W29-08 -- SA Web-Estate CMS Exposure Sweep

P3 -- MEDIUM: proactive; targets the asset class nobody owns

Hypothesis: The organisation owns or sponsors internet-facing websites -- microsites, campaign pages, event portals, legacy domains -- that are not in any asset inventory, run an unpatched CMS with vulnerable third-party extensions, and have no assigned owner. This week's four Joomla KEV entries make that population directly exploitable.

MITRE ATT&CK: T1595.002 (Active Scanning: Vulnerability Scanning), T1590 (Gather Victim Network Information), T1190 (Exploit Public-Facing Application).

IOCs: Behavioural, not atomic: hostnames resolving to organisation-controlled or agency-controlled IP space that are absent from the CMDB; Joomla or WordPress fingerprints on .co.za and .gov.za properties; extension versions below SP Page Builder 6.6.2 or Page Builder CK 3.6.0; shared-hosting neighbours under the same account.

Data Sources: DNS zone exports, certificate-transparency logs, external attack-surface management tooling, Shodan/Censys, registrar and hosting-account inventories, agency contracts.

Detection Guidance: Enumerate every hostname in the DNS zone and every certificate issued for the domain. Fingerprint the CMS and extension versions on each. Assign a named owner to every property; anything without an owner should be taken offline rather than patched. Where sites are agency-hosted, obtain written confirmation of extension versions and patch status this week -- the KEV deadline for the second Joomla pair is 13 July.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

1. Run a website inventory before you run anything else: pull the DNS zone and certificate-transparency records, fingerprint every CMS, and identify Joomla installations with SP Page Builder, Page Builder CK, iCagenda or Balbooa Forms. Patch, remove or take offline. Then hunt -- for the bhup.php web shell, for new PHP files under media directories, and for Super User accounts created outside a change window. The persistence account survives the patch.

2. Assume compromise on exposed ColdFusion: CVE-2026-48282 was exploited under two hours after disclosure and the KEV deadline lapsed on 10 July. Apply the 30 June update, disable RDS in production, and run a compromise assessment on any instance that was internet-facing and unpatched between 30 June and 7 July. A patch applied after exploitation is remediation of the vector, not of the intrusion.

3. Close the exploited-but-unlisted gap: Gitea CVE-2026-20896 (upgrade to 1.26.3/1.26.4, restrict trusted proxies, strip X-WEBAUTH-USER at the edge, rotate CI secrets) and Oracle EBS CVE-2026-46817 (sweep /OA_HTML/ibytransmit POSTs from 27 June, patch at the 21 July CPU, de-expose). Neither is in the KEV catalogue and both are being exploited now. Rebuild your patch SLA around exploitation evidence, not catalogue membership.

4. Recalibrate the KEV clock: remediation deadlines under BOD 26-04 are running at roughly three days, not the three weeks assumed under BOD 22-01. Any internal SLA that says 'patch KEV entries within 21 days' is now three weeks behind the federal standard it was copied from. Re-baseline, and re-check the Ubiquiti UniFi OS and Lantronix entries -- they were due 26 June, not 14 July, and are overdue.

Management (CISO / Board)

1. The R44.1 million number should replace the R10 million number in every business case: the average South African breach now costs more than four times POPIA's maximum administrative fine. If security investment has been argued on the basis of avoiding a regulatory penalty, the argument has been made against a number that is four times too small. Reframe on total breach cost -- remediation, churn, downtime, reputational drag -- and use the 3,219 notifications and 268-per-month run rate as the base rate.

2. Ask who owns the company's websites: this week's dominant exploitation wave targets an asset class that most boards have never been shown -- outsourced marketing sites, event pages, legacy microsites. Ask for the list. If nobody can produce one within a day, that is the finding. Sites without an owner should be decommissioned, not patched.

3. Do not read regulatory silence as regulatory tolerance: the Information Regulator has published nothing since 2 June, and the TransUnion / Experian section 59 responses have passed their deadline with no public outcome. Enforcement capacity is constrained, not absent -- and the infringement notices already issued are being pursued through the courts where unpaid. Organisations should keep breach-notification readiness current rather than tracking the Regulator's news cycle.

4. Third-party and supply-chain attestation, again: the week's exposures ran through hosting providers, extension vendors, an RMM platform and a source-code host. Ask for written confirmation of patch status this week from your web-hosting agency (Joomla extension versions), your MSP (SimpleHelp patched and tokens rotated), and your development partners (Gitea version and secret rotation). One email, three answers, and it should not take a week to get them.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH -- 9th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for a ninth consecutive week (5 July - 12 July 2026). No new South African incident was recorded in the window, and on a purely domestic reading the case for a downgrade to MEDIUM is arguable. It is rejected for three reasons: the exploitation tempo against internet-facing assets tripled, with six KEV additions all rated 9.8 or above on three-day fuses; four of those six sit in a content-management stack that is disproportionately represented in the unmanaged South African web estate and is therefore an unmeasured domestic exposure rather than an absent one; and the published breach series -- 3,219 notifications in the financial year, about 268 a month -- demonstrates that the absence of leak-site postings is a reporting artefact, not a quiet threat environment.

Rationale

- **Six KEV additions in seven days, none below CVSS 9.8:** triple the prior week's volume, with roughly three-day remediation deadlines under BOD 26-04. Two deadlines (10 July) have already lapsed and one (13 July) falls the day this report is read.
- **The exploitation frontier moved to unmanaged assets:** four Joomla third-party extension file-upload RCEs target websites, not servers -- the asset class with no inventory, no monitoring and no assigned owner in most South African organisations.
- **Time-to-exploit collapsed:** Adobe ColdFusion CVE-2026-48282 (CVSS 10.0) was exploited under two hours after disclosure; Page Builder CK was exploited within hours of its fix shipping; SP Page Builder was exploited as a zero-day. Change-approval cycles are now slower than the attack.
- **Two CVSS 9.8 flaws are being exploited with no KEV listing at all:** Gitea CVE-2026-20896 and Oracle EBS CVE-2026-46817 (day 15). Catalogue-driven patching leaves both open.
- **The domestic quiet is not measured:** zero new SA leak-site listings for six weeks against 268 breach notifications a month means the leak-site series is a floor on SA ransomware activity, not a measurement.
- **Carryovers remain unresolved, not retired:** Profmed / PPSHA scope (four schemes unconfirmed, including the SANDF RFMCF), AVBOB undetermined at six weeks, the Standard Bank leak unresolved, TransUnion / Experian responses overdue with no public outcome, and #OpSouthAfrica dormant with DCS data still held.
- **Regulatory enforcement is thin:** the Information Regulator has published nothing since 2 June, and the R44.1m average breach cost now exceeds POPIA's R10m fine ceiling by more than four times -- the deterrent sits below the harm.

Next-Week Watch (W30)

- **Joomla wave, SA victims:** first named South African victim of the SP Page Builder / Page Builder CK / iCagenda / Balbooa exploitation, most plausibly a municipality, NGO or SME on shared hosting. Also watch for further Joomla extension KEV additions -- this cluster is not finished.
- **13 July KEV deadline:** iCagenda CVE-2026-48939 and Balbooa Forms CVE-2026-56291 fall due the day this report is published; watch for post-deadline exploitation reporting.
- **Patch Tuesday, 14 July:** volume, zero-days, and whether SQL Server enters rotation. Oracle Critical Patch Update follows 21 July -- the likely fix vehicle for EBS CVE-2026-46817.
- **Oracle EBS CVE-2026-46817:** whether CISA finally adds it to the KEV catalogue (day 15 and counting), and whether any victim is named. Same question for Gitea CVE-2026-20896.
- **TransUnion SA / Experian SA:** the section 59 responses are now overdue; any Information Regulator statement, enforcement notice or first publication since 2 June.
- **Profmed / PPSHA:** confirmation or exclusion of the other four administered schemes, especially the SANDF Regular Force Medical Continuation Fund.
- **ICASA / Session Telecoms:** progress of the operator's review application and whether the 'industry-wide' SIM-boxing allegation draws a regulator or MTN response.

- **ransomware.live**: whether the six-week SA quiet streak ends; and whether any SA victim surfaces through breach notification rather than leak site.
- **FIC**: first cross-border cash conveyance seizure or operational statement, and the 31 July second-batch RCR deadline.

12. OSINT SOURCES CONSULTED

The following open-source intelligence sources were consulted in the preparation of this report. All sources are TLP:WHITE and publicly accessible. Numbers 1-29 correspond to the inline footnote citations used throughout this report; each unique source appears exactly once. All cited URLs were retrieved and verified on 12 July 2026. Two fetch-environment limitations are disclosed for transparency. First, cisa.gov blocks direct automated retrieval from our environment: all CISA KEV facts in this report (CVE identifiers, addition dates, remediation deadlines and required actions) are therefore anchored to multiple independent fetched secondary sources quoting the CISA alerts -- primarily items 1, 2, 3 and 5 -- rather than to the catalogue itself. Second, mybroadband.co.za is likewise blocked; no MyBroadband claim is relied upon in this edition. Where a claim could not be verified against a fetched source it has been excluded or explicitly flagged in the text.

1. Security Affairs -- U.S. CISA adds Adobe ColdFusion, Joomla! Page Builder, Langflow, and Joomla! Shaper SP Page Builder flaws to its Known Exploited Vulnerabilities catalog (7 July 2026) -- <https://securityaffairs.com/194927/hacking/u-s-cisa-adds-adobe-coldfusion-joomla-page-builder-langflow-and-joomlshaper-sp-page-builder-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
2. The Hacker News -- CISA adds 4 actively exploited Adobe ColdFusion and Joomla! extension flaws to KEV catalog (7 July 2026) -- <https://thehackernews.com/2026/07/cisa-adds-4-actively-exploited-adobe.html>
3. Security Affairs -- U.S. CISA adds iCagenda and Balboa Forms flaws to its Known Exploited Vulnerabilities catalog (10 July 2026) -- <https://securityaffairs.com/195164/security/u-s-cisa-adds-icagenda-and-balboa-forms-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
4. Security Affairs -- Adobe ColdFusion flaw CVE-2026-48282 now exploited in the wild (5 July 2026) -- <https://securityaffairs.com/194837/hacking/adobe-coldfusion-flaw-cve-2026-48282-now-exploited-in-the-wild.html>
5. Senserva -- CISA KEV Additions (July 2026): Vulnerabilities Exploited This Week (checked 12 July 2026) -- <https://senserva.com/exploited-this-week.html>
6. Security Affairs -- Critical Gitea Docker bug under active exploitation exposes repositories and secrets (6 July 2026) -- <https://securityaffairs.com/194902/hacking/critical-gitea-docker-bug-under-active-exploitation-exposes-repositories-and-secrets.html>
7. Security Affairs -- Ubiquiti patches critical UniFi OS flaws allowing command injection and privilege escalation (8 July 2026) -- <https://securityaffairs.com/194978/security/ubiquiti-patches-critical-unifi-os-flaws-allowing-command-injection-and-privilege-escalation.html>
8. Security Affairs -- Update now: critical Zimbra Classic Web Client flaw could expose mailboxes (10 July 2026) -- <https://securityaffairs.com/195130/hacking/update-now-critical-zimbra-classic-web-client-flaw-could-expose-mailboxes.html>
9. Help Net Security -- July 2026 Patch Tuesday forecast (10 July 2026) -- <https://www.helpnetsecurity.com/2026/07/10/july-2026-patch-tuesday-forecast/>
10. Security Affairs -- U.S. CISA adds Ubiquiti UniFi OS and Lantronix EDS5000 plugin flaws to its Known Exploited Vulnerabilities catalog (23 June 2026) -- <https://securityaffairs.com/194142/security/u-s-cisa-adds-ubiquiti-unifi-os-and-lantronix-eds5000-plugin-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
11. IOL Business Report -- South Africa's data breaches could be costing the economy R142 billion a year (7 July 2026) -- <https://iol.co.za/business-report/economy/2026-07-07-south-africas-data-breaches-could-be-costing-the-economy-r142-billion-a-year/>

12. TechFinancials -- South Africa's costly data breaches: 1.81% GDP loss and the avoidable own-goals costing the economy (6 July 2026) -- <https://techfinancials.co.za/2026/07/06/south-africas-costly-data-breaches-1-81-gdp-loss-and-the-avoidable-own-goals-costing-the-economy/>
13. Sowetan -- Rise in data breaches puts influencers and everyday users at risk (8 July 2026) -- <https://www.sowetan.co.za/news/2026-07-08-rise-in-data-breaches-puts-influencers-and-everyday-users-at-risk/>
14. Engineering News -- POPIA five years later: why is nobody being held accountable? (6 July 2026) -- <https://www.engineeringnews.co.za/article/popia-five-years-later-why-is-nobody-being-held-accountable-2026-07-06>
15. ITWeb -- InfoReg exposes POPIA violators as data breaches mount (14 November 2025) -- <https://www.itweb.co.za/article/infoereg-exposes-popia-violators-as-data-breaches-mount/kLgB17ezby5M59N4>
16. Information Regulator (South Africa) -- Media statements (checked 12 July 2026; most recent statement dated 2 June 2026) -- <https://infoeregulator.org.za/media-statements/>
17. TechFinancials -- ICASA imposes multiple sanctions on SA telecoms provider (9 July 2026) -- <https://techfinancials.co.za/2026/07/09/icasa-imposes-multiple-sanctions-on-sa-telecoms-provider/>
18. TechFinancials -- Session Telecoms slaps regulator with legal challenge, alleges industry-wide fraud cover-up in R6m penalty row (9 July 2026) -- <https://techfinancials.co.za/2026/07/09/session-telecoms-slaps-regulator-with-legal-challenge-alleges-industry-wide-fraud-cover-up-in-r6m-penalty-row/>
19. Engineering News -- Domestic, foreign travellers must now declare cash of more than R100 000 -- FIC (1 July 2026) -- <https://www.engineeringnews.co.za/article/domestic-foreign-travellers-must-now-declare-cash-of-more-than-r100-000-fic-2026-07-01>
20. ransomware.live -- South Africa victim map (checked 12 July 2026; 109 cumulative SA victims) -- <https://www.ransomware.live/map/ZA>
21. Data Breaches Digest -- Week 28 2026 edition, covering 6 - 12 July 2026 (checked 12 July 2026) -- <https://www.dbdigest.com/2026/07/data-breaches-digest-week-28-2026.html>
22. Breachsense -- Data breaches, July 2026 (checked 12 July 2026) -- <https://www.breachsense.com/breaches/2026/july/>
23. Quasar CyberTech Q-Pulse -- Multiple ransomware groups target diverse organizations in June and July 2026 (6 July 2026) -- <https://qpulse.quasarcybertech.com/news/4219/multiple-ransomware-groups-target-diverse-organizations-in-june-and-july-2026>
24. BleepingComputer -- Police arrest 5,800 suspects in global anti-fraud crackdown (9 July 2026) -- <https://www.bleepingcomputer.com/news/security/police-arrests-5-800-suspects-in-global-anti-fraud-crackdown/>
25. INTERPOL -- Over 5,800 arrests, USD 293 million intercepted in global fraud bust (July 2026) -- <https://www.interpol.int/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust>
26. BleepingComputer -- Ryuk ransomware member pleads guilty in the US, faces 15 years in prison (10 July 2026) -- <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-member-pleads-guilty-in-the-us-faces-15-years-in-prison/>
27. ITWeb -- Security section index (checked 12 July 2026; no SA incident reporting dated 5 - 12 July 2026) -- <https://www.itweb.co.za/categories/pXnWJadMba7bjO1e>
28. TechCentral -- News index (checked 12 July 2026; no SA incident reporting dated 5 - 12 July 2026) -- <https://techcentral.co.za/category/news/>
29. IOL -- Cyber attack tag index (checked 12 July 2026; most recent tagged item dated 15 June 2026) -- <https://iol.co.za/tags/cyber-attack/>

This report is classified TLP:WHITE. It may be distributed without restriction. Information sourced from publicly available OSINT. No classified or restricted sources were used. Where a claim rests on a single source or a threat-actor assertion, it is explicitly rated PROBABLE or CLAIMED in the text. Prepared by Digital Progression | dpcyber.co.za | DP-CTI-2026-W29 | Published Monday 13 July 2026