



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief -- Week 31 | 19 July - 26 July 2026

THREAT LEVEL: HIGH

TLP:WHITE

Report ID: SA-CTI-2026-W31 | Classification: TLP:WHITE

Published Monday 27 July 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 (W31)**
- 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 -- 11th consecutive week (19 July - 26 July 2026)

Story 1 -- Rectron confirmed a breach, named a ransomware group, and notified the regulator: last week's 'probable' is this week's confirmed supply-chain incident. Rectron, one of South Africa's four largest technology distributors, published a notice acknowledging that unlawful third-party access to its network was identified on 15 July 2026, that personal information of customers, employees and suppliers was accessed and potentially exfiltrated, that the Information Regulator has been notified, and that the attacker is suspected to be affiliated with the DragonForce ransomware group.⁵⁶ The company is in recovery, liaising with the board of parent Mustek, and has engaged forensic specialists.⁶ This upgrades INC-2026-W30-05 from PROBABLE to CONFIRMED and moves the exposure into the IT channel: Rectron distributes hardware and enterprise security products to a large share of the South African reseller base, so the follow-on risk is fraud and impersonation against partners during the disruption window.

Story 2 -- the ransomware.live South African tally jumped to 115 as the six-week reporting lag cleared, and a new Qilin victim appeared. The ransomware.live country-statistics page reported 115 cumulative South African victims across 50 groups when retrieved on 26 July, against the 109 this report has cited since early June.⁹ The step of six is a catch-up in the aggregator's country attribution rather than six fresh compromises in one week -- exactly the lag this report has flagged since W25, now visible in the data. Qilin listed a new South African business-services victim, Recsa (recsasec.org), on 22 July.⁸ Meanwhile the two open W30 claims resolved in opposite directions: DragonForce's Isegen claim drew a public denial from the company, which says its investigation found no evidence of unauthorised access,⁷ while BE Travel's Arcus Media countdown expired on 21 July with no confirmed publication and no further statement.¹⁰

Story 3 -- six more KEV additions, an actively exploited SharePoint flaw that steals cryptographic keys, and the largest Oracle patch release ever recorded. CISA added six vulnerabilities to the KEV catalogue on 21-22 July, including a WordPress Core pair (CVE-2026-63030 and CVE-2026-60137) that chains into the pre-authentication 'wp2shell' remote code execution, Langflow CVE-2026-0770 (RCE as root), Check Point SmartConsole CVE-2026-16232 (an unauthenticated attacker obtains a full admin token) and SharePoint CVE-2026-50522, which is under mass exploitation to steal server machine keys in a single request -- meaning patching alone is insufficient and machine keys must be rotated.²³ Oracle's 21 July Critical Patch Update was the largest in its history at 1,235 CVEs, with 410 patches for E-Business Suite of which 45 are remotely exploitable without authentication.¹

KPI Dashboard

Metric	Current (W31)	Prior (W30)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (11th week)	FLAT
ransomware.live SA cumulative	115	109	+6 (lag clearance)	UP
New SA leak-site claims	1	3	-2	DOWN
Confirmed SA incidents	1	2	-1	DOWN
W30 incidents upgraded to CONFIRMED	1 (Rectron)	n/a	+1	UP
New CISA KEV additions	6	10	-4	DOWN
Oracle CPU CVEs (21 Jul)	1,235	n/a	record CPU	UP
IR public statements in window	0	0	0	FLAT
Weeks since last IR publication	8	7	+1	UP

W31 KEY FRAMING: W31 is a resolution week. Three of the four domestic threads this report opened in W30 closed with harder facts: Rectron confirmed a breach and named DragonForce, Isegen denied compromise, and BE Travel's leak countdown lapsed without confirmed publication. Only the Profmed/PPSHA scope remains genuinely open. The headline number -- the ransomware.live tally moving from 109 to 115 -- is the clearest vindication yet of a position this report has held for six weeks: the flat country total was a measurement lag, not a quiet threat environment, and the correction confirms real activity was accumulating unseen. Externally the pressure held rather than rose: six KEV additions against ten the prior week, but with two that defeat patch-only remediation (SharePoint machine-key theft and the Check Point admin-token bypass) and a record 1,235-CVE Oracle release that most South African ERP estates cannot absorb in one cycle. The actionable centre of gravity this week is the IT supply chain and the perimeter appliance.

TOP 3 ACTIONS THIS WEEK

1. Patch AND rotate for SharePoint CVE-2026-50522 and Check Point CVE-2026-16232 -- these two defeat patch-only remediation. SharePoint CVE-2026-50522 (CVSS 9.8, KEV due 25 July, now lapsed) is under mass exploitation to steal server machine keys in a single request following a public PoC on 20 July; apply the update and then rotate ASP.NET machine keys, because a stolen key lets an attacker forge access after patching. For Check Point SmartConsole CVE-2026-16232 (CVSS 9.3), block the six published attacker IPs (151.241.99.207, 151.241.99.233, 158.62.198.182, 192.142.10.99, 139.28.37.250, 194.213.18.137), patch, and review for unauthorised administrative tokens.

2. Harden your IT-distributor and reseller relationships in light of the confirmed Rectron breach. Rectron confirmed personal data was accessed and potentially exfiltrated and named DragonForce as the suspected actor. Until the company completes its investigation, verify any 'updated banking details' or invoice correspondence bearing the Rectron brand through a known contact, inventory and rotate credentials and API keys shared with the distributor's ordering and licensing platforms, and brief finance and procurement teams that distributor-branded fraud is the most likely near-term follow-on.

3. Close the WordPress wp2shell chain and the AD FS deadline. The WordPress Core pair CVE-2026-63030 (CVSS 9.8) and CVE-2026-60137 (CVSS 5.9) chains into pre-authentication RCE on WordPress 6.9.x and 7.0.x; forced auto-updates were enabled but self-hosted and managed estates must confirm they applied. This is the same unmanaged-web-estate exposure flagged in W29 and W30, now with a working public exploit. Separately, AD FS CVE-2026-56155 (KEV due 28 July) falls the day after this report is read -- patch it now, not on the deadline, and review AD FS administrative group membership and token-signing certificate history.

1. Tenable -- Oracle July 2026 Critical Patch Update Addresses 1,235 CVEs (21 July 2026) --

<https://www.tenable.com/blog/oracle-july-2026-critical-patch-update-addresses-1235-cves>

2. Security Affairs -- U.S. CISA adds DD-WRT, Langflow and WordPress flaws to its Known Exploited Vulnerabilities catalog (21 July 2026)

-- <https://securityaffairs.com/195782/security/u-s-cisa-adds-dd-wrt-langflow-and-wordpress-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

3. Security Affairs -- U.S. CISA adds Microsoft SharePoint and Check Point SmartConsole flaws to its KEV catalog (22 July 2026) -- <https://securityaffairs.com/195889/security/u-s-cisa-adds-microsoft-sharepoint-and-check-point-smartconsole-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

5. Hypertext (htxt.co.za) -- Leading South African tech distributor Rectron suffers cyberattack (24 July 2026) --

<https://htxt.co.za/2026/07/leading-south-african-tech-distributor-suffers-cyberattack/>

6. IT-Online -- Rectron goes into recovery mode after cyber attack (22 July 2026) --

<https://it-online.co.za/2026/07/22/rectron-goes-into-recovery-mode-after-cyber-attack/>

7. ChemAnalyst -- South African chemical producer Isegen targeted by DragonForce; company denies compromise (20 July 2026) -- [http://www.chemanalyst.com/NewsAndDeals/NewsDetails/south-african-chemical-giant-isegen-targeted-by-notorious-ransomware-group-43409](https://www.chemanalyst.com/NewsAndDeals/NewsDetails/south-african-chemical-giant-isegen-targeted-by-notorious-ransomware-group-43409)

8. DeXpose -- Qilin ransomware strikes Recsa in South Africa (July 2026; claim posted 22 July) --

<https://www.dexpose.io/qilin-ransomware-strikes-recsa-in-south-africa/>

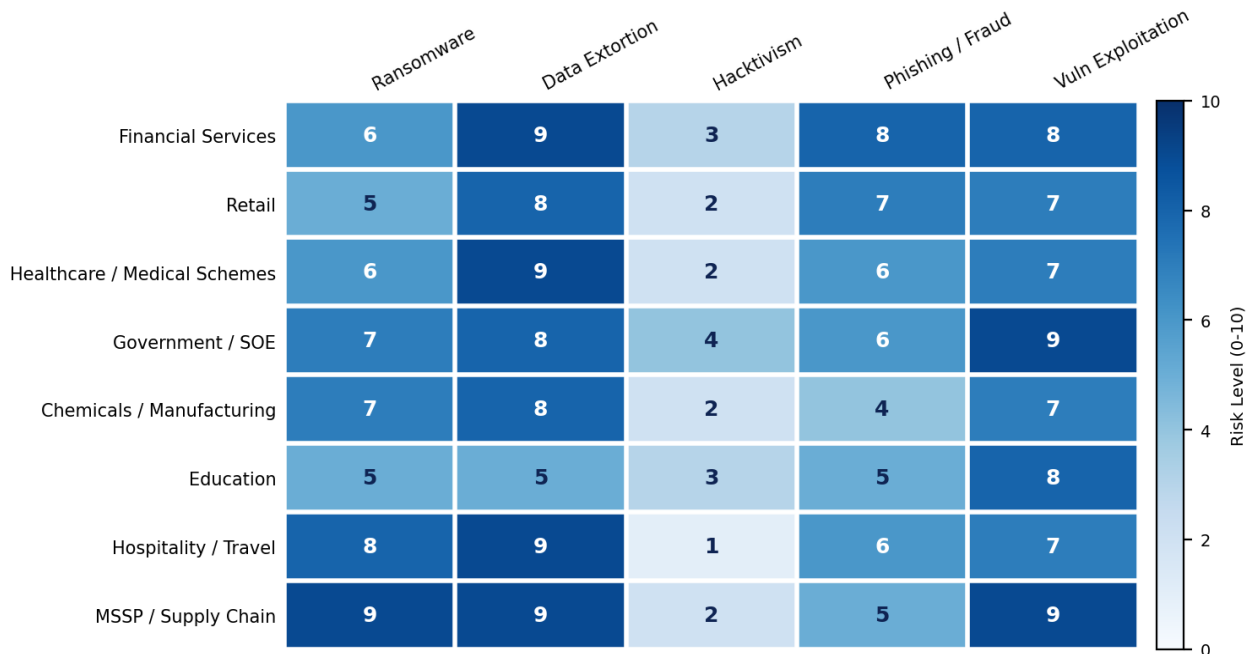
9. Ransomware.live -- South Africa country statistics (retrieved 26 July 2026; 115 cumulative victims, 50 groups) --

<https://www.ransomware.live/countrystats/ZA>

10. Ransomware.live -- South Africa victim map, BE Travel / Arcus Media listing (retrieved 26 July 2026; deadline 21 July, publication unconfirmed) -- <https://www.ransomware.live/map/ZA>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W31 (19 July - 26 July 2026)



Methodology: Risk levels are assessed using: (a) confirmed incidents in the reporting window; (b) credible threat-actor claims against the sector; (c) exposure to vulnerabilities under active exploitation; (d) regulatory and enforcement pressure. Scale: Critical 9-10 = active exploitation or confirmed breach in the window; High 7-8 = credible active threat; Medium 4-6 = elevated baseline; Low 1-3 = standard posture.

MSSP / Supply Chain is the top-rated row this week at 9 on Ransomware and 9 on Data Extortion, driven by the confirmed Rectron breach: a top-four national technology distributor with data accessed and potentially exfiltrated, DragonForce suspected, and a channel-wide fraud follow-on.⁵ It holds 9 on Vulnerability Exploitation because the week's exploited flaws -- Check Point SmartConsole, SonicWall SMA 1000, SharePoint -- concentrate in managed-service and mid-market estates.³⁴ **Hospitality / Travel** holds at 8-9 on the BE Travel incident, whose leak countdown lapsed without confirmed publication.¹⁰ **Government / SOE** remains at 9 on Vulnerability Exploitation on the standing Gauteng jobs portal breach and the density of exploited enterprise flaws in state estates.¹³ **Chemicals / Manufacturing** eases to 7 on Ransomware: Isegen publicly denied compromise, so the DragonForce claim is downgraded in weight though not dismissed.⁷ **Financial Services** holds at 9 on Data Extortion on the unresolved Standard Bank / Liberty listing.⁹ **Hacktivism** stays low: #OpSouthAfrica has shown no activity since May.

11. Information Regulator (South Africa) -- Media statements (checked 26 July 2026; no statement in the window) -- <https://infoeregulator.org.za/media-statements/>

12. Information Regulator (South Africa) -- Enforcement notices (checked 26 July 2026; no notice in the window) -- <https://infoeregulator.org.za/enforcement-notice/>

3. TOP SA INCIDENTS (W31)

Week 31 (19 July - 26 July 2026) is defined by resolution of the prior week's open threads rather than a fresh wave. Four items are recorded: one CONFIRMED breach (Rectron, upgraded from W30), one new CLAIMED leak-site listing (Recsa / Qilin), and two carryover resolutions moving in opposite directions (Isegen denied, BE Travel countdown lapsed). The ransomware.live South African country-statistics total was 115 across 50 groups when retrieved on 26 July, up from the 109 cited since early June -- a lag-clearance discussed in Section 6.⁹ Confidence ratings: CONFIRMED (victim or regulator acknowledgment, or two independent sources), PROBABLE (single credible source), CLAIMED (threat-actor assertion only).

3.1 INC-2026-W31-01 -- Rectron Confirmed Breach; DragonForce Suspected [CONFIRMED] (upgrade of INC-2026-W30-05)

Sector	Technology Distribution / IT Supply Chain (Rectron, subsidiary of Mustek)
Date	Unlawful access identified 15 July 2026; public notice 22-24 July 2026
Confirmed	Unlawful third-party access to the network; personal information of customers, employees and suppliers accessed and potentially exfiltrated; Information Regulator notified; forensic specialists engaged; recovery ongoing and liaison with the Mustek board
Attribution	Attacker suspected by Rectron to be affiliated with the DragonForce ransomware group; no leak-site listing naming Rectron observed by 26 July
Significance	Channel-wide: Rectron distributes hardware and enterprise security products (Microsoft, Bitdefender, Acronis) to a large share of the SA reseller base; a live POPIA section 22 case
Confidence	CONFIRMED (victim acknowledgment on the company's own notice, corroborated by two independent trade outlets)

Rectron's public notice, quoted in trade coverage, states that unlawful third-party access to its network was identified on 15 July 2026, that personal information relating to customers, employees and suppliers was accessed and potentially exfiltrated, that the Information Regulator has been notified, and that the suspected attacker is affiliated with the DragonForce ransomware group.⁵ IT-Online corroborates that the company entered recovery mode with containment and forensic work ongoing, and that it is liaising with the Mustek board.⁶ This confirms and upgrades INC-2026-W30-05, which this report rated PROBABLE while the outage cause was unacknowledged. The DragonForce link is notable: the same operation claimed Isegen South Africa on 15 July (Section 3.3), placing two suspected DragonForce events against South African targets in a single fortnight. Practical exposure for the channel is unchanged from the W30 assessment but now confirmed: resellers and their customers should treat distributor-branded banking-change or invoice correspondence as high-risk pending Rectron's all-clear, and rotate any credentials, API keys or integrations shared with the distributor's ordering and licensing platforms. No ransomware leak-site listing for Rectron had appeared by 26 July, consistent with either an active negotiation or a data-theft-without-publication posture.

3.2 INC-2026-W31-02 -- Qilin Claims Recsa (recsasec.org) [CLAIMED]

Sector	Business Services (recsasec.org)
Date	Leak-site listing 22 July 2026
Claimed	Data theft with publication threatened; victim listed on the Qilin leak site
Corroboration	Single threat-intelligence aggregator (DeXpose); no victim statement located; not yet independently corroborated
Actor	Qilin -- prolific ransomware-as-a-service operation, second-most-active group globally in June 2026 and historically active against African targets
Confidence	CLAIMED (threat-actor assertion only, single aggregator source)

Qilin listed the South African business-services entity Recsa (recsasec.org) on its leak site on 22 July.⁸ No sample has been verified and Recsa has made no public statement, so this remains an uncorroborated actor claim and should not be reported internally as a confirmed breach. It is the only genuinely new South African leak-site claim in the window and is consistent with Qilin's continued high tempo: the group was the second-most-active ransomware operation worldwide in June 2026 and has a documented African footprint. Organisations with Recsa in their supply chain should request a written status update rather than waiting for any publication of the claimed dataset.

3.3 INC-2026-W31-03 -- Isegen Denies DragonForce Compromise [CARRYOVER; victim denial]

Sector	Chemicals / Manufacturing (KwaZulu-Natal; isegen.co.za)
Date	DragonForce claim 15 July 2026; Isegen denial reported 20 July 2026
Victim position	Isegen states its internal investigation found no evidence of unauthorised access, compromised systems or stolen information; operations fully functional
Actor position	DragonForce claims 234.63 GB exfiltrated and threatens publication on 6 August 2026; listing live on the leak site since 14 July
Assessment	Direct conflict between a single-outlet victim denial and an uncorroborated actor claim; unresolved pending proof or publication
Confidence	Claim CLAIMED; denial PROBABLE (single credible outlet)

Isegen has publicly denied the DragonForce claim recorded in W30, stating that its investigation found no evidence of unauthorised access, compromised systems or stolen information, and that operations are fully functional.⁷ DragonForce maintains the claim, now specifying 234.63 GB of data and a publication deadline of 6 August 2026. This is a genuine evidentiary conflict, not a resolution: a victim denial and an actor claim can both be sincere when a claim is fabricated or recycled, or when a victim has not yet detected an intrusion. The report holds the claim at CLAIMED and records the denial at PROBABLE, and will re-assess if DragonForce publishes on or before 6 August. Organisations should neither treat the Isegen data as confirmed-stolen nor dismiss the possibility while the 6 August deadline stands.

3.4 INC-2026-W31-04 -- BE Travel / Arcus Media: Leak Countdown Lapsed [CARRYOVER; publication unconfirmed]

Sector	Hospitality / Travel with government supply-chain reach (betravel.co.za)
Date	Arcus Media publication deadline 21 July 2026; status checked 26 July 2026
Status	The Arcus Media listing still shows the 21 July deadline with no leak-size or 'published' marker and no proof pack; no further statement from BE Travel or the Housing Development Agency
Prior confidence	Incident itself CONFIRMED in W30 (victim information-officer acknowledgment); the question this week is whether exfiltrated data was published
Confidence	Incident CONFIRMED (W30); publication UNCONFIRMED as of 26 July

The Arcus Media leak-site entry for BE Travel, checked on 26 July, still carries the 21 July deadline without any indication that data was published, and no proof pack has appeared.¹⁰ The underlying ransomware incident remains CONFIRMED from the victim's own information officer in W30; only the publication outcome was open, and it is now most likely one of three states -- a private settlement, an ongoing negotiation, or a bluff. The government supply-chain exposure noted in W30 (BE Travel holds the Housing Development Agency travel tender) is unchanged: absent publication, there is no evidence that HDA-related data has been released, but equally no confirmation that it has not. Organisations exposed through the HDA contract should continue to monitor and should have used the two weeks since disclosure to confirm what personal data the agency holds on their staff.

Carryover Status (checked 26 July 2026)

Profmed / PPS Healthcare Administrators: no development and no Information Regulator statement; the administered-scheme scope (KeyHealth, SEDMED, De Beers Benefit Society, SANDF RFMCF) remains neither confirmed nor excluded at eight weeks -- now the single most durable unresolved South African exposure. **Gauteng e-Government jobs portal breach:** no new development beyond the 14 July disclosure; no Information Regulator statement on the 283-record identity-document exposure.¹³ **Standard Bank / Liberty (Prinz Eugen / ROOTBOY):** listing unchanged and unretracted.⁹ **AVBOB Mutual Assurance:** approximately eight weeks post-incident with no leak-site claim; UNDETERMINED. **#OpSouthAfrica (Nullsec Nigeria / Anonymous Nigeria):** no activity since May 2026; Department of Correctional Services data remains in actor hands -- dormant, not resolved. **SAPS Western Cape POPIA breach and Tembisa Hospital prosecution:** no published outcome. **ICASA / Session Telecoms:** no published progress.

13. ITWeb -- Gauteng ignored AG warning before job portal breach (14 July 2026; W30 carryover) -- <https://www.itweb.co.za/article/gauteng-ignored-ag-warning-before-job-portal-breach/Pero3MZ31O3qQb6m>

4. THREAT ACTORS

4.1 DragonForce [CONFIRMED activity against SA]

DragonForce is now the most significant ransomware actor against South Africa this fortnight, named by Rectron as the suspected group behind a confirmed breach of a top-four technology distributor, and the claimant against Isegen South Africa.⁵⁷ The operation runs a data-theft-and-extortion model and its affiliates have been observed abusing signed but vulnerable Microsoft-ecosystem drivers to disable endpoint protection -- a technique that surfaces in telemetry as unexpected kernel driver loads shortly before mass file access. The Rectron case (confirmed compromise, regulator notified, no leak-site listing yet) and the Isegen case (claim disputed by the victim) show the group's two public postures side by side: quiet negotiation after a confirmed intrusion, and loud pre-publication pressure on a contested one. Assessment: highest-priority ransomware actor for South African distribution, manufacturing and industrial estates; two suspected events against SA targets in one fortnight is a meaningful concentration.

4.2 Qilin [CLAIMED activity against SA]

Qilin listed a new South African business-services victim, Recsa, on 22 July.⁸ The group was the second-most-active ransomware operation worldwide in June 2026 and has a long African targeting history. Qilin operates a mature ransomware-as-a-service programme with a well-run leak site and affiliate structure, and open-source reporting in the window links Qilin affiliates to exploitation of edge-device vulnerabilities for initial access. Assessment: a persistent, high-tempo threat to South African organisations across sectors; the Recsa claim should be treated as a live risk pending corroboration.

4.3 SonicWall SMA 1000 Zero-Day Operator (UTA0533) [CONFIRMED exploitation]

Volatility has attributed the SonicWall SMA 1000 zero-day exploitation (CVE-2026-15409, CVSS 10.0; CVE-2026-15410, CVSS 7.2) to a threat cluster tracked as UTA0533, active since around 22 June 2026.⁴ The tradecraft is now documented: exploitation for root access, deployment of an ORANGETAIL webshell, and LDAP credential sniffing to harvest directory credentials from the appliance's authentication traffic. SonicWall has confirmed the exploitation and a proof-of-concept has been published by Rapid7, which broadens the pool of capable attackers. Assessment: this is no longer a single-operator zero-day but a documented campaign with public tooling; any South African organisation that had an SMA 1000 exposed before mid-July must assume potential pre-patch compromise and hunt for ORANGETAIL and anomalous LDAP query patterns, not merely patch.

4.4 Check Point SmartConsole Exploiters [CONFIRMED exploitation; UNATTRIBUTED]

An unattributed operator is actively exploiting CVE-2026-16232 (CVSS 9.3), an improper authentication flaw in Check Point SmartConsole that lets an unauthenticated attacker obtain a full administrative token.³ Check Point has confirmed active exploitation and published six attacker IP addresses as indicators (151.241.99.207, 151.241.99.233, 158.62.198.182, 192.142.10.99, 139.28.37.250, 194.213.18.137). The target is the management plane of a security product: an attacker with a SmartConsole admin token can alter firewall policy, which makes this a high-leverage foothold rather than a single-host compromise. Assessment: relevant to any South African organisation running Check Point management infrastructure; the published IPs give an immediate, atomic detection and blocking opportunity that is rare this week.

4.5 SharePoint Machine-Key Theft Cluster [CONFIRMED exploitation]

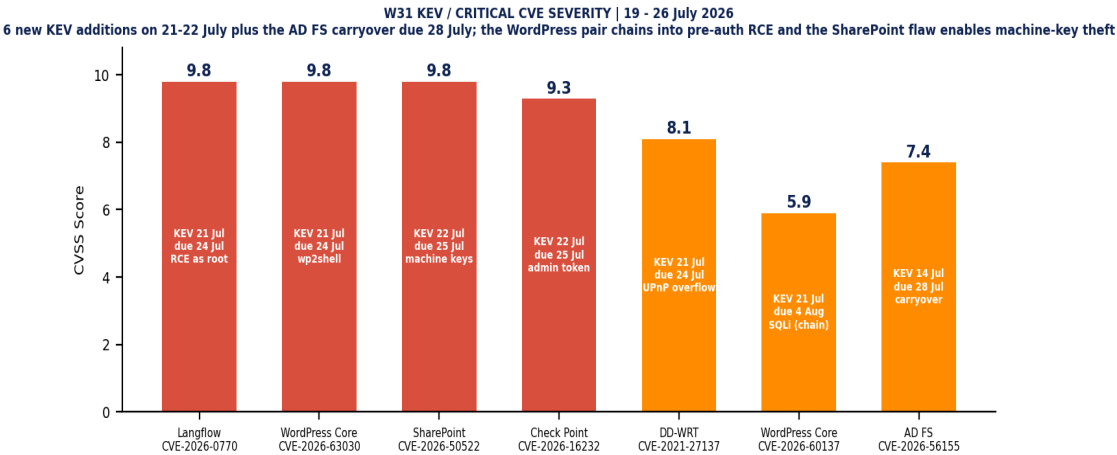
CVE-2026-50522 (CVSS 9.8), a SharePoint deserialization flaw demonstrated at Pwn2Own and patched in the 14 July release, came under mass exploitation after a public proof-of-concept on 20 July, with honeypot operators observing attackers stealing SharePoint server machine keys in a single request.³ Stolen machine keys allow an attacker to forge authentication and view-state payloads that remain valid after the server is patched, which is why the required response is patch-and-rotate rather than patch alone. This is the fourth distinct SharePoint issue this report has tracked in four weeks, against a persistent backdrop of Storm-2603 and Warlock ransomware activity against on-premises SharePoint. Assessment: on-premises SharePoint remains the single most repeatedly weaponised enterprise application in the current series; any South African organisation still self-hosting it must rotate machine keys now.

4. Security Affairs -- Volexity uncovers zero-day campaign targeting SonicWall SMA 1000 VPN appliances (UTA0533) (July 2026) -- <https://securityaffairs.com/195626/hacking/volexity-uncovers-zero-day-campaign-targeting-sonicwall-vpn-appliances.html>

5. CRITICAL VULNERABILITIES & CISA KEV

Six vulnerabilities entered the CISA KEV catalogue on 21 and 22 July 2026, against ten the previous week.²³ Volume fell but two of the six defeat patch-only remediation. SharePoint CVE-2026-50522 (CVSS 9.8, due 25 July) is exploited to steal machine keys, so remediation requires key rotation as well as the patch; Check Point SmartConsole CVE-2026-16232 (CVSS 9.3, due 25 July) yields a full admin token, so remediation should include hunting for tokens already issued. The 21 July batch is dominated by the WordPress Core pair -- CVE-2026-63030 (CVSS 9.8) and CVE-2026-60137 (CVSS 5.9) -- which chains into the pre-authentication 'wp2shell' RCE against WordPress 6.9.x and 7.0.x, alongside Langflow CVE-2026-0770 (CVSS 9.8, RCE as root) and an older DD-WRT UPnP buffer overflow, CVE-2021-27137 (CVSS 8.1). Separately, Oracle's 21 July Critical Patch Update was the largest in the company's history at 1,235 CVEs across 1,449 patches, with 410 patches for E-Business Suite of which 45 are remotely exploitable without authentication -- a remediation load that will outrun most South African ERP change cycles.¹ The one carryover deadline inside the window is AD FS CVE-2026-56155, due 28 July, the day after this report is read.

W31 KEV / Critical CVE Severity Overview -- 6 New KEV Adds 21-22 July Plus AD FS Carryover



W31 CISA KEV / Critical CVE Tracking (new adds 21-22 July plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-50522	Microsoft SharePoint Server	9.8	Deserialization RCE	25 Jul	KEV 22 Jul. Mass exploitation after 20 Jul PoC; steals machine keys in one request. PATCH AND ROTATE machine keys.
CVE-2026-16232	Check Point SmartConsole	9.3	Improper auth	25 Jul	KEV 22 Jul. Unauth attacker obtains full admin token. Six attacker IPs published as IoCs. Hunt for issued tokens.
CVE-2026-0770	Langflow	9.8	RCE (root)	24 Jul	KEV 21 Jul. Remote code execution as root; AI/LLM orchestration platform. Continuation of Langflow exploitation since W28.
CVE-2026-63030	WordPress Core	9.8	Interpretation conflict	24 Jul	KEV 21 Jul. Chains with CVE-2026-60137 for pre-auth 'wp2shell' RCE on WP 6.9.x/7.0.x. Forced auto-updates enabled.
CVE-2026-60137	WordPress Core	5.9	SQL injection	4 Aug	KEV 21 Jul. Second half of the wp2shell chain; longer fuse but part of an active pre-auth RCE. Confirm on self-hosted estates.
CVE-2021-27137	DD-WRT	8.1	UPnP buffer overflow	24 Jul	KEV 21 Jul. Legacy router firmware; relevant to SOHO and branch estates running DD-WRT. Old CVE, active exploitation.
CVE-2026-56155	Microsoft AD Federation Services	7.4	Priv escalation	28 Jul	Carryover (KEV 14 Jul). Actively exploited; pairs with RCE in ransomware intrusions. Deadline the day after publication.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	OVERDUE +9. Zero-day by UTA0533 since 22 Jun; ORANGETAIL webshell, LDAP credential sniffing; Rapid7 PoC public. Assume compromise.
CVE-2026-46817	Oracle E-Business Suite	n/a	Improper privilege mgmt	18 Jul	OVERDUE +8. Exploited since 27 Jun; fixed in May 2026 CPU. Re-verify against the 21 Jul CPU's 410 EBS patches.

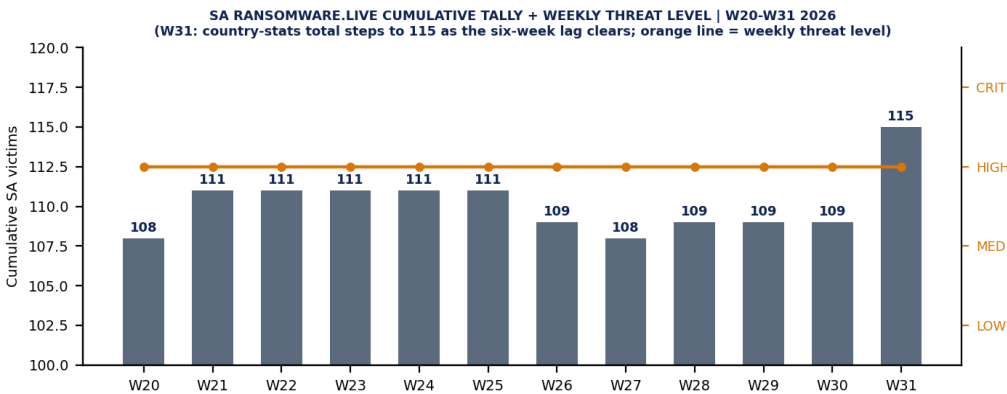
CVE-2026-58644	Microsoft SharePoint Server	9.8	Deserialization RCE	19 Jul	OVERDUE +7. Verify remediation alongside CVE-2026-50522 and rotate machine keys across all SharePoint hosts.
----------------	-----------------------------	-----	---------------------	--------	--

Pattern note: W31's signal is that the patch is no longer the finish line. Two of the six new KEV entries -- SharePoint machine-key theft and the Check Point admin-token bypass -- leave an attacker with durable, forgeable access that survives patching, so the remediation verb is rotate-and-hunt, not patch. This is a meaningful escalation in required effort: a KEV deadline met by patching may still leave a compromised estate. Combined with a record 1,235-CVE Oracle release, the operational reality for a South African security team is that the volume of remediation and the depth of each remediation both rose at once. Prioritise the two rotate-and-hunt items and the still-overdue SonicWall SMA 1000 zero-day above raw CVSS ordering.

1. Tenable -- Oracle July 2026 Critical Patch Update Addresses 1,235 CVEs (21 July 2026) -- <https://www.tenable.com/blog/oracle-july-2026-critical-patch-update-addresses-1235-cves>

6. RANSOMWARE LANDSCAPE

The ransomware.live South African country-statistics page reported 115 cumulative victims across 50 groups when retrieved on 26 July 2026, up from the 109 this report has cited since early June.⁹ The step of six is the single most important ransomware data point of the week, and it is not six fresh compromises: it is the aggregator's country attribution catching up. Only one genuinely new South African leak-site claim was posted in the window -- Qilin's listing of Recsa on 22 July.⁸ The other five of the six-victim delta reflect earlier compromises being belatedly country-tagged, exactly the lag this report has argued since W25 makes the country total a trailing floor rather than a live measurement. The correction vindicates that reading: activity was accumulating unseen behind a static headline number. A data-quality caveat compounds it -- the ransomware.live /map/ZA page continues to serve a stale cached render showing 109, while the /countrystats/ZA page shows the current 115; this report uses the country-stats figure and flags the discrepancy so it does not propagate into automated feeds as a phantom delisting.⁹¹⁰



Baseline (W30)	109 cumulative SA victims (country map), carried since early June
Current (W31)	115 cumulative SA victims across 50 groups (country-stats page, retrieved 26 July 2026)

Genuinely new claims	1 in window: Recsa / Qilin (22 Jul, CLAIMED)
Delta explanation	+6 is aggregator lag-clearance (earlier compromises belatedly country-tagged), not six new week-of compromises
Carryover resolutions	Isegen / DragonForce denied by victim; BE Travel / Arcus Media countdown lapsed without confirmed publication; Rectron confirmed (no leak-site listing yet)
Data-quality caveat	ransomware.live /map/ZA serves a stale 109 cache; /countrystats/ZA shows current 115 -- country-stats used
Threat-level drivers	Confirmed distributor breach (DragonForce); new Qilin victim; two rotate-and-hunt KEV items; record Oracle CPU

Group notes: DragonForce -- confirmed against Rectron and claiming Isegen; two suspected SA events in a fortnight (Section 4.1). **Qilin** -- new Recsa claim; second-most-active group globally in June, persistent African targeting (Section 4.2). **Arcus Media** -- BE Travel countdown lapsed 21 July without confirmed publication; monitor for delayed release.¹⁰ **Prinz Eugen / ROOTBOY** -- Standard Bank / Liberty listing unchanged and unretracted.⁹ **The Gentlemen** -- no new SA victim this week but retains the top global position from June and holds Sunspray Food from April; remains an elevated watch for SA manufacturing and food production.

7. OSINT EXPOSURE & ATTACK SURFACE

IT distribution channel -- the confirmed Rectron exposure

The confirmed Rectron breach is the week's most consequential attack-surface finding for South African organisations, because the exposure is transitive: a distributor breach reaches every reseller and end customer that integrates with the distributor's ordering, licensing and support systems, and every finance team that pays distributor invoices.⁵⁶ Rectron has confirmed personal data of customers, employees and suppliers was accessed and potentially exfiltrated. Exposure action: inventory every integration, shared credential and API key connecting your environment to Rectron; rotate anything stale or over-privileged; apply out-of-band verification to any change in distributor banking or payment details; and monitor for lookalike domains and distributor-branded phishing while the disruption is public knowledge and therefore a credible pretext.

Check Point SmartConsole and SonicWall SMA 1000 -- management-plane and edge exposure

Two exploited perimeter and management-plane flaws this week give South African defenders rare atomic indicators. Check Point published six attacker IPs for CVE-2026-16232 exploitation (151.241.99.207, 151.241.99.233, 158.62.198.182, 192.142.10.99, 139.28.37.250, 194.213.18.137), which can be blocked and hunted immediately.³ SonicWall SMA 1000 exploitation by UTA0533 deploys an ORANGETAIL webshell and sniffs LDAP credentials, and a public Rapid7 PoC now widens the attacker pool.⁴ Exposure action: identify Check Point management infrastructure and SMA 1000 appliances by external and internal scan, block the published IPs, patch, and for the SMA 1000 treat any pre-mid-July internet exposure as a suspected compromise -- hunt for ORANGETAIL and anomalous LDAP query volumes rather than relying on the patch.

WordPress and on-premises SharePoint -- the recurring unmanaged and self-hosted estate

The wp2shell WordPress Core chain (CVE-2026-63030 plus CVE-2026-60137) now has a working public exploit against WordPress 6.9.x and 7.0.x, extending the unmanaged-web-estate exposure this report has tracked since W29 into core WordPress rather than third-party plugins.² Forced auto-updates were enabled, but self-hosted and agency-managed sites must confirm they applied. On-premises SharePoint remains the most repeatedly weaponised enterprise application in the series, with CVE-2026-50522 now stealing machine keys; every self-hosting South African organisation should patch and rotate ASP.NET machine keys across all SharePoint hosts.³ Exposure action: re-run the owned-domain and CMS inventory from W30, add SharePoint machine-key rotation to the SharePoint control set, and confirm WordPress core versions across every hosted property.

8. REGULATORY & POLICY

Rectron as a live POPIA section 22 case [CONFIRMED]

Rectron's confirmation that it has notified the Information Regulator makes this the clearest live POPIA section 22 breach-notification case in the current series, and one to watch precisely because the notification is on the record.⁵ Section 22 requires notification to the Regulator and to affected data subjects as soon as reasonably possible after a compromise, and Rectron's public statement establishes both that a reportable compromise occurred and that the company has engaged the process. For other accountable parties the transferable point is procedural: Rectron has modelled the expected sequence -- identify, contain, notify the Regulator, engage forensics, communicate -- and its handling will become a reference case for how a large South African distributor discharges section 22. A public, prompt notification is itself a mitigating posture.

Information Regulator: eight weeks without a public statement [CONFIRMED]

The Information Regulator's media-statements and enforcement-notice pages, both checked on 26 July 2026, show no new publication in the window and nothing since the early-June items this report has tracked.¹¹¹² That is eight weeks without a published media statement, across a period now containing a confirmed provincial-government identity-document breach (Gauteng) and a confirmed national distributor breach with regulator notification (Rectron). As stated in prior editions, the absence of publication is not evidence of inactivity -- investigations are not published in progress -- but it leaves regulated entities without a recent published precedent against which to calibrate their own section 22 decisions. The conservative reading of section 22 remains the safe default.

FIC Directive 11 RCR deadline, 31 July 2026 [forward-looking]

The Financial Intelligence Centre's Risk and Compliance Return second-batch deadline falls at 17:00 on Friday 31 July 2026 for the relevant accountable-institution categories, and the FIC has signalled that late or non-submission attracts administrative sanction. This is a forward-looking compliance date rather than a threat-intelligence finding, carried from prior editions, and is recorded here so that affected South African accountable institutions -- non-casino gambling, legal practitioners, estate agents, high-value goods dealers and the other listed categories -- treat the deadline as firm. Boards should confirm submission status this week rather than assuming compliance.

9. WEEKLY THREAT HUNT & IOCs

Seven hunt missions are active for W31. This is an unusually indicator-rich week: unlike recent editions dominated by behavioural-only hunts, three missions carry atomic indicators -- six Check Point attacker IPs, the SonicWall ORANGETAIL webshell, and the SharePoint machine-key-theft request pattern. Three P1 missions address the rotate-and-hunt SharePoint and Check Point flaws and the SonicWall SMA 1000 campaign; two P2 missions cover the WordPress wp2shell chain and IT-distributor supply-chain exposure following the confirmed Rectron breach; two P3 missions address Langflow RCE and DragonForce ransomware pre-encryption behaviour. A machine-readable indicator export accompanies this report (iocs_w31.csv).

TH-2026-W31-01 -- SharePoint CVE-2026-50522
Machine-Key Theft Hunt

P1 -- CRITICAL: CVSS 9.8; mass exploitation post-PoC; KEV due 25 Jul (LAPSED); patch insufficient

Hypothesis: An unauthenticated attacker sends a single crafted request to an on-premises SharePoint server exploiting the CVE-2026-50522 deserialization flaw to extract the server's ASP.NET machine keys. With the machine key, the attacker forges __VIEWSTATE and authentication payloads that remain valid after patching, giving durable access. Patching without rotating machine keys leaves the estate compromised.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1552 (Unsecured Credentials), T1606.001 (Forge Web Credentials: Web Cookies), T1505.003 (Web Shell), T1078 (Valid Accounts).

IOCs: SharePoint machine-key theft request pattern (single POST to SharePoint endpoints returning serialized objects); anomalous __VIEWSTATE payloads validating against a known machine key; w3wp.exe spawning cmd.exe or powershell.exe; new .aspx/.ashx files under LAYOUTS or content web roots; requests correlating with the 20 July PoC signature.

Data Sources: SharePoint ULS logs, IIS logs, EDR process-creation telemetry, file-integrity monitoring on SharePoint web roots, WAF logs.

Detection Guidance: Patch immediately -- the 25 July deadline has passed -- and ROTATE ASP.NET machine keys across every SharePoint host, then invalidate existing sessions. Hunt backwards to 20 July for the theft request and for forged-viewstate activity. Because CVE-2026-58644 (overdue since 19 July) affects the same product, treat machine-key rotation as an estate-wide action, not a per-CVE one.

**TH-2026-W31-02 -- Check Point SmartConsole
CVE-2026-16232 Admin-Token Hunt****P1 -- CRITICAL: CVSS 9.3; confirmed
exploitation; six attacker IPs published;
KEV due 25 Jul (LAPSED)**

Hypothesis: An unauthenticated attacker exploits an improper authentication flaw in Check Point SmartConsole to obtain a full administrative token, then uses management-plane access to read or alter firewall policy. Because the compromise is of the security-management plane, its blast radius is the entire protected network rather than one host.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1556 (Modify Authentication Process), T1562.001 (Impair Defenses), T1098 (Account Manipulation).

IOCs: Attacker IPs (block and alert): 151.241.99.207, 151.241.99.233, 158.62.198.182, 192.142.10.99, 139.28.37.250, 194.213.18.137. Also: unrecognised SmartConsole administrative sessions or tokens; firewall policy changes with no change-ticket; new or modified administrator accounts on the management server.

Data Sources: Check Point management server and SmartConsole audit logs, firewall policy change history, perimeter and management-segment netflow, SIEM alerts on the published IPs.

Detection Guidance: Block the six published IPs at the perimeter and alert on any historical connection from them. Patch the SmartConsole / management server -- the 25 July deadline has passed. Enumerate and validate every administrative token and account, and review firewall policy change history for unauthorised modifications since mid-July. Treat any confirmed policy change from these IPs as a full management-plane compromise.

**TH-2026-W31-03 -- SonicWall SMA 1000 UTA0533 /
ORANGETAIL Hunt****P1 -- CRITICAL: CVSS 10.0; UTA0533
zero-day since 22 Jun; Rapid7 PoC
public; KEV OVERDUE +9**

Hypothesis: The UTA0533 cluster exploits CVE-2026-15409 (SSRF) and CVE-2026-15410 (code injection) on SMA 1000 appliances for root access, deploys an ORANGETAIL webshell, and sniffs LDAP credentials from the appliance's authentication traffic. A public Rapid7 PoC has broadened the attacker pool. Any appliance internet-exposed before mid-July should be treated as potentially compromised regardless of current patch status.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1040 (Network Sniffing), T1552 (Unsecured Credentials), T1133 (External Remote Services).

IOCs: ORANGETAIL webshell artefacts on the appliance filesystem; anomalous or high-volume LDAP queries originating from the appliance; outbound HTTP from the appliance to internal RFC1918 or cloud-metadata addresses; new administrator accounts; VPN sessions from ASNs with no business rationale; session tokens valid across a firmware upgrade.

Data Sources: SMA appliance system and access logs, AMC audit logs, LDAP/directory server query logs, firewall egress logs, DMZ netflow, IdP logs for accounts authenticating through the appliance.

Detection Guidance: Patch -- the 17 July deadline lapsed nine days ago -- then treat as suspected compromise: hunt for ORANGETAIL, review appliance and LDAP logs from 22 June onward for credential-sniffing activity, rotate all credentials and tokens reachable through the appliance, and rebuild from known-good firmware if ORANGETAIL or anomalous LDAP activity is found.

TH-2026-W31-04 -- WordPress wp2shell Pre-Auth RCE Chain Hunt

P2 -- HIGH: CVE-2026-63030 + CVE-2026-60137 chain; public exploit; WP 6.9.x/7.0.x

Hypothesis: An unauthenticated attacker chains CVE-2026-63030 (interpretation conflict) and CVE-2026-60137 (SQL injection) against WordPress Core 6.9.x or 7.0.x to achieve pre-authentication remote code execution ('wp2shell'), then deploys a webshell for credential capture, malware distribution or pivot into the corporate network. Forced auto-updates were enabled but self-hosted and agency-managed estates may not have applied.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1059 (Command and Scripting Interpreter), T1105 (Ingress Tool Transfer), T1078 (Valid Accounts).

IOCs: Unexpected .php files in WordPress plugin, theme or upload directories; PHP files with recent modification timestamps; POST requests with SQL-injection or encoded payloads to wp-login or REST endpoints; new administrator accounts; web server process spawning shell children; outbound connections from the web host to non-CDN destinations.

Data Sources: Web server access and error logs, WordPress core-version inventory, filesystem integrity monitoring of web roots, CMS user and audit tables, hosting-provider logs, egress netflow.

Detection Guidance: Confirm WordPress Core is patched to the fixed 6.9.x/7.0.x release across every owned property, including agency-managed sites. Inspect web directories for unexpected files and review logs for the injection pattern. If a webshell is found, trace the initial exploitation, look for lateral movement and new accounts, and restore from a known-good backup. Re-run the owned-domain and CMS inventory from W30 if not already complete.

TH-2026-W31-05 -- IT Distributor Supply-Chain Hunt (Confirmed Rectron Breach)

P2 -- HIGH: confirmed distributor breach; data exfiltration; DragonForce suspected

Hypothesis: With the Rectron breach now confirmed and personal data accessed and potentially exfiltrated, reseller and end-customer integrations with the distributor -- ordering portals, licensing provisioning, B2B APIs, EDI links and shared credentials -- constitute a potential downstream attack path, and distributor-branded correspondence is a high-credibility phishing and payment-fraud pretext during the disruption window.

MITRE ATT&CK: T1195 (Supply Chain Compromise), T1199 (Trusted Relationship), T1566.002 (Spearphishing Link), T1078 (Valid Accounts), T1534 (Internal Spearphishing).

IOCs: Rectron-branded password-reset, banking-detail-change or invoice emails from 15 July 2026 onward; logins to reseller portal accounts from unfamiliar sources; anomalous activity on API keys or service accounts shared with Rectron; licensing or provisioning changes not initiated by your own staff; lookalike domains registered against the Rectron brand.

Data Sources: Email gateway telemetry, finance/AP change-request logs, reseller portal access logs, API gateway logs for distributor integrations, IdP logs for shared or federated accounts, domain-monitoring feeds.

Detection Guidance: Verify any payment-detail or ordering change through a known Rectron contact on an existing number, not details in new correspondence. Inventory and rotate credentials, API keys and integrations shared with the distributor. Brief finance teams that distributor-branded invoice and banking-change requests are high-risk pending Rectron's all-clear. Watch for a possible DragonForce leak-site listing of Rectron and for the claimed data appearing for sale.

TH-2026-W31-06 -- Langflow CVE-2026-0770 RCE Hunt

P3 -- MEDIUM: CVSS 9.8, RCE as root; KEV due 24 Jul (LAPSED); AI-platform exposure

Hypothesis: An attacker exploits CVE-2026-0770 in the Langflow AI/LLM orchestration platform to achieve remote code execution as root. Langflow instances are frequently stood up by data-science and AI teams outside standard change control and asset inventory, so the exposure is often unmanaged. This continues the Langflow exploitation this report has tracked intermittently since W28.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1610 (Deploy Container), T1068 (Exploitation for Privilege Escalation), T1552 (Unsecured Credentials).

IOCs: HTTP requests to Langflow endpoints from unexpected sources; Langflow process spawning shell children; outbound connections from Langflow hosts to unfamiliar destinations; new files or containers on the host; access to model, API-key or secrets material stored by the platform.

Data Sources: Langflow application and host logs, container-runtime logs, EDR telemetry on AI/ML hosts, egress netflow, secrets-manager access logs, cloud audit logs for AI workloads.

Detection Guidance: Identify Langflow instances -- including shadow deployments by data-science teams -- and patch to the fixed release; the 24 July deadline has passed. Confirm no instance is internet-reachable without authentication and a WAF. Rotate any API keys or model credentials the platform can access. Bring AI/LLM platforms into the standard asset inventory and vulnerability-management scope.

TH-2026-W31-07 -- DragonForce Ransomware Pre-Encryption Behaviour Hunt

P3 -- MEDIUM: confirmed against Rectron; SA distribution/manufacturing targeting

Hypothesis: DragonForce, confirmed against Rectron and claiming Isegen, operates a data-theft-and-extortion model and its affiliates abuse signed but vulnerable Microsoft-ecosystem drivers to disable endpoint protection before mass file access. The hypothesis is that a DragonForce affiliate present in a South African distribution or manufacturing network will exhibit driver-abuse and defense-impairment behaviour ahead of exfiltration.

MITRE ATT&CK: T1486 (Data Encrypted for Impact), T1567 (Exfiltration Over Web Service), T1562.001 (Impair Defenses), T1543.003 (Create or Modify System Process: Windows Service), T1055 (Process Injection).

IOCs: Unexpected kernel driver loads, particularly signed-but-vulnerable drivers, shortly before bulk file access; endpoint-protection service stops or tamper events; large staged archives; outbound transfers to file-sharing or cloud-storage services; mass file reads across shares in a short window.

Data Sources: EDR process and driver-load telemetry, Windows Security and Sysmon logs, DLP and egress netflow, file-server access auditing, endpoint-protection tamper alerts.

Detection Guidance: Enable and alert on vulnerable-driver blocklists (Microsoft recommended driver block rules). Hunt for driver-load events immediately preceding defense-impairment and bulk file access. For distribution and manufacturing estates specifically, given two suspected DragonForce events against SA targets this fortnight, prioritise this hunt and validate offline, immutable backups.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Treat the two rotate-and-hunt KEV items as this week's top priority above raw CVSS.** For SharePoint CVE-2026-50522, patch and rotate ASP.NET machine keys across every SharePoint host, then hunt for forged viewstate back to 20 July. For Check Point CVE-2026-16232, block the six published attacker IPs, patch, and validate every administrative token. A met patch deadline does not close either of these.
- 2. Run the confirmed-Rectron supply-chain hunt now.** Inventory integrations, shared credentials and API keys connecting to Rectron; rotate stale or over-privileged ones; alert on Rectron-branded banking-change and invoice correspondence from 15 July; and watch for a DragonForce leak-site listing of Rectron and for the claimed data appearing for sale.
- 3. Close the still-overdue SonicWall SMA 1000 zero-day as a compromise, not a patch.** Exploitation by UTA0533 with a public PoC and an ORANGETAIL webshell means any pre-mid-July internet exposure warrants a hunt for ORANGETAIL and anomalous LDAP query volumes, credential rotation, and appliance rebuild if artefacts are found.
- 4. Confirm WordPress Core versions across every owned property.** The wp2shell chain has a working public exploit against 6.9.x and 7.0.x; forced auto-updates help but self-hosted and agency-managed sites must be verified. Re-use the owned-domain and CMS inventory from W30.
- 5. Bring AI/LLM platforms into scope.** Langflow CVE-2026-0770 (RCE as root) is exploited and often runs as a shadow deployment outside asset inventory. Find Langflow instances, patch, remove internet exposure, and rotate any credentials they can reach.

Management (CISO / Board)

- 1. The Rectron breach is the supply-chain lesson made concrete.** A confirmed compromise at a top-four distributor reaches every organisation that buys or integrates through it. Identify your critical technology suppliers and confirm, in writing, what data they hold on you, what their breach-notification obligation to you is, and how you would verify a payment-detail change during their incident. Rectron modelled prompt section 22 notification -- use it as the reference for what good looks like.
- 2. Patch deadlines are no longer a sufficient board metric.** Two of this week's exploited flaws leave forgeable access after patching. Ask your team not just 'are we within KEV deadlines' but 'for the rotate-and-hunt items, have we rotated keys and hunted for prior compromise'. The honest answer is the one that matters.
- 3. The ransomware.live jump from 109 to 115 is a measurement correction, not a surge -- but the correction is the point.** The domestic threat did not spike this week; six weeks of accumulating activity became visible at once. Do not over-react to the number, but do register that the quiet headline counts of June and early July were understated, and calibrate risk accordingly.

4. Register the regulatory silence as a planning assumption. The Information Regulator has published nothing for eight weeks despite two confirmed breaches in the period. Plan on the conservative reading of section 22 notification; the commercial case for controls does not rest on the fine.

5. Confirm the 31 July FIC RCR submission this week. For affected accountable-institution categories the second-batch Risk and Compliance Return is due at 17:00 on 31 July with administrative sanction for non-submission. Confirm status now rather than assuming compliance.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH -- 11th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for an eleventh consecutive week (19 July - 26 July 2026). W31 is a consolidation of W30's escalation rather than a further step: the confirmed Rectron breach, the new Qilin victim, and two rotate-and-hunt KEV items sustain the level, while the ransomware tally's jump to 115 confirms that prior weeks understated real activity. Escalation to CRITICAL was considered and rejected -- no systemically important institution (bank, telco, grid, major SOE) is confirmed compromised, the new leak-site claim is uncorroborated, and the KEV volume fell week on week. De-escalation is not supportable while a top-four distributor breach is live, two rotate-and-hunt flaws are being exploited, and a SonicWall zero-day remains overdue.

Rationale

- **A confirmed national supply-chain breach:** Rectron acknowledged unlawful access, data accessed and potentially exfiltrated, regulator notified, DragonForce suspected -- upgrading last week's PROBABLE and putting a top-four distributor and its reseller channel at risk.
- **Two exploited flaws that survive patching:** SharePoint CVE-2026-50522 (machine-key theft) and Check Point CVE-2026-16232 (admin-token bypass) require rotate-and-hunt, so a met patch deadline may still leave a compromised estate.
- **The ransomware tally corrected upward to 115:** a +6 lag-clearance confirming six weeks of understated activity, plus a genuinely new Qilin victim (Recsa) -- the quiet was a measurement artefact, as this report has argued since W25.
- **A record Oracle release compounding remediation load:** 1,235 CVEs on 21 July with 410 E-Business Suite patches (45 unauth-remote), on top of six new KEV items -- both the volume and the depth of remediation rose at once.
- **An overdue perimeter zero-day with public tooling:** SonicWall SMA 1000 exploitation by UTA0533 (ORANGETAIL webshell, LDAP credential sniffing) is nine days past its KEV deadline with a public Rapid7 PoC.
- **Carryovers resolving unevenly:** Isegen denied compromise, BE Travel's countdown lapsed without confirmed publication, but Profmed/PPSHA scope is unresolved at eight weeks and #OpSouthAfrica remains dormant with DCS data still held.

- **Regulatory signal still absent:** the Information Regulator has published nothing for eight weeks across two confirmed breaches.

Next-Week Watch (W32)

- **Rectron:** completion of the forensic investigation, scope and nature of exfiltrated data, any DragonForce leak-site listing, service-restoration confirmation, and any Information Regulator or Mustek statement.
- **Isegen / DragonForce, 6 August deadline:** whether DragonForce publishes the claimed 234.63 GB, which would resolve the victim-denial-versus-actor-claim conflict.
- **BE Travel / Arcus Media:** any delayed publication of the exfiltrated data or any Housing Development Agency statement.
- **AD FS CVE-2026-56155, 28 July deadline:** post-deadline exploitation reporting and whether a paired RCE emerges as ZDI anticipates.
- **SharePoint machine-key theft:** named South African victims and whether the machine-key-rotation message reaches self-hosting SA estates before compromise.
- **Check Point SmartConsole:** further attacker infrastructure, named victims, and whether the six published IPs expand.
- **Qilin / Recsa:** corroboration or denial, and any publication of the claimed dataset.
- **ransomware.live:** whether the country-stats total moves again and whether the /map/ZA cache is refreshed to match.
- **FIC:** the 31 July RCR second-batch deadline outcome and any enforcement posture.
- **Information Regulator:** any publication after eight weeks, particularly on Rectron or the Gauteng e-Government breach.

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 1-15 correspond to the inline footnote citations; each unique source appears exactly once. Every cited URL was directly retrieved and confirmed to contain the claim attributed to it, on 26 July 2026. Transparency notes: cisa.gov blocks direct automated retrieval from our environment, so all CISA KEV facts are anchored to fetched secondary sources quoting the CISA alerts directly (items 1, 2 and 3). The ransomware.live /map/ZA page (item 10) served a stale cached render showing 109; the current figure of 115 is taken from the /countrystats/ZA page (item 9), and the discrepancy is analysed in Section 6. The FIC Directive 11 RCR deadline referenced in Section 8 is a forward-looking compliance date carried from prior editions and is not presented as a new sourced claim.

1. Tenable -- Oracle July 2026 Critical Patch Update Addresses 1,235 CVEs (21 July 2026) -- <https://www.tenable.com/blog/oracle-july-2026-critical-patch-update-addresses-1235-cves>

2. Security Affairs -- U.S. CISA adds DD-WRT, Langflow and WordPress flaws to its Known Exploited Vulnerabilities catalog (21 July 2026) -- <https://securityaffairs.com/195782/security/u-s-cisa-adds-dd-wrt-langflow-and-wordpress-flaws-to-its-known-exploited-vulnerabilities-catalog.html>

3. Security Affairs -- U.S. CISA adds Microsoft SharePoint and Check Point SmartConsole flaws to its KEV catalog (22 July 2026) -- <https://securityaffairs.com/195889/security/u-s-cisa-adds-microsoft-sharepoint-and-check-point-smartconsole-flaws-to-it-s-known-exploited-vulnerabilities-catalog.html>
4. Security Affairs -- Volexity uncovers zero-day campaign targeting SonicWall SMA 1000 VPN appliances (UTA0533) (July 2026) -- <https://securityaffairs.com/195626/hacking/volexity-uncovers-zero-day-campaign-targeting-sonicwall-vpn-appliances.html>
5. Hypertext (htxt.co.za) -- Leading South African tech distributor Rectron suffers cyberattack (24 July 2026) -- <https://htxt.co.za/2026/07/leading-south-african-tech-distributor-suffers-cyberattack/>
6. IT-Online -- Rectron goes into recovery mode after cyber attack (22 July 2026) -- <https://it-online.co.za/2026/07/22/rectron-goes-into-recovery-mode-after-cyber-attack/>
7. ChemAnalyst -- South African chemical producer Isegen targeted by DragonForce; company denies compromise (20 July 2026) -- <https://www.chemanalyst.com/NewsAndDeals/NewsDetails/south-african-chemical-giant-isegen-targeted-by-notorio-us-ransomware-group-43409>
8. DeXpose -- Qilin ransomware strikes Recsa in South Africa (July 2026; claim posted 22 July) -- <https://www.dexpose.io/qilin-ransomware-strikes-recsa-in-south-africa/>
9. Ransomware.live -- South Africa country statistics (retrieved 26 July 2026; 115 cumulative victims, 50 groups) -- <https://www.ransomware.live/countrystats/ZA>
10. Ransomware.live -- South Africa victim map, BE Travel / Arcus Media listing (retrieved 26 July 2026; deadline 21 July, publication unconfirmed) -- <https://www.ransomware.live/map/ZA>
11. Information Regulator (South Africa) -- Media statements (checked 26 July 2026; no statement in the window) -- <https://infoeregulator.org.za/media-statements/>
12. Information Regulator (South Africa) -- Enforcement notices (checked 26 July 2026; no notice in the window) -- <https://infoeregulator.org.za/enforcement-notice/>
13. ITWeb -- Gauteng ignored AG warning before job portal breach (14 July 2026; W30 carryover) -- <https://www.itweb.co.za/article/gauteng-ignored-ag-warning-before-job-portal-breach/Pero3MZ3IO3qQb6m>
14. MyBroadband -- SA company that books flights for HDA hit by ransomware attack (BE Travel; 18 July 2026) -- <https://mybroadband.co.za/news/security/658327-south-african-company-that-books-flights-for-agency-in-r29-6-billion-government-department-hit-by-ransomware-attack.html>
15. MyBroadband -- One of South Africa's largest technology distributors suffers crippling network outage allegedly due to cyberattack (Rectron; 19 July 2026) -- <https://mybroadband.co.za/news/security/658697-one-of-south-africas-largest-technology-distributors-suffers-crippling-network-outage-allegedly-due-to-cyberattack.html>

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. Single-source and threat-actor claims are rated PROBABLE or CLAIMED in the text. SA-CTI-2026-W31 | Published Monday 27 July 2026