



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief -- Week 30 | 12 July - 19 July 2026

THREAT LEVEL: HIGH

TLP:WHITE

Report ID: SA-CTI-2026-W30 | Classification: TLP:WHITE

Published Monday 20 July 2026

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard
- 2. Threat Landscape Heatmap
- 3. Top SA Incidents (W30)
- 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 -- 10th consecutive week (12 July - 19 July 2026)

Story 1 -- Microsoft shipped the largest single-month patch release in its history, and two of the flaws were already being exploited. The July 2026 Patch Tuesday on 14 July carried 621 Microsoft CVEs, 63 of them Critical, a figure the Zero Day Initiative notes already puts the 2026 year-to-date count above every full-year total of the last two decades.¹ Two were flagged under active exploitation: CVE-2026-56155, an elevation-of-privilege flaw in Active Directory Federation Services, and CVE-2026-56164, a SharePoint Server missing-authentication flaw rated only CVSS 5.3. Both entered the CISA KEV catalogue on 14 July.² The 5.3 score is the operational lesson of the week: severity-threshold patching would have deprioritised a vulnerability that is unauthenticated, needs no user interaction, and is being used now. The highest-rated fix of the month, CVE-2026-57092 in Windows VMSwitch at CVSS 9.9, permits escape from a guest virtual machine to the Hyper-V host and is not in the KEV at all.¹

Story 2 -- South Africa's six-week quiet ended emphatically: two confirmed domestic incidents, one probable breach at a major technology distributor, and a government supply-chain angle. BE Travel (Baithaupi Executive Travel) confirmed through its information officer that it suffered a ransomware incident on 4 July 2026, that Arcus Media has made contact, and that POPIA notifications have gone to affected data subjects -- and the company holds the active 36-month travel-management tender for the Housing Development Agency, the state property developer inside the R29.6-billion Department of Human Settlements budget.¹⁶⁹ Gauteng MEC for e-Government Bonginkosi Dhlamini separately confirmed, in a written legislature reply reported 14 July, that the provincial e-Recruitment jobs portal was breached, exposing 283 application records including certified South African ID copies and proof of residence, via a compromised non-privileged account against an unfunded, unimplemented Auditor-General control.⁷ And on 16-17 July Rectron, one of the country's four largest technology distributors, closed every office nationwide during a network outage that sources attribute to a breach -- the company has neither confirmed nor denied a cyberattack.¹⁷ Leak-site claims completed the picture: Isegen South Africa by DragonForce on 15 July,⁸ and suppcentersa.com by m3rx on 17 July with a country attribution this report treats as unreliable.¹⁰

Story 3 -- Ten KEV additions in seven days, and an allied cyber agency put a name to the web-estate campaign this report flagged last week. CISA added ten vulnerabilities to the KEV catalogue between 13 and 16 July, against six the prior week.²³⁴⁵ Oracle E-Business Suite CVE-2026-46817, tracked in this report as exploited-but-uncatalogued since W28, was finally added on 15 July with an 18 July deadline.³ On 13 July the Australian Signals Directorate published an alert on a large-scale global campaign deploying webshells through 17 named CVEs across WordPress plugins, Joomla, Craft CMS, MaxSite and MetInfo, explicitly noting small and medium businesses among the victims.⁶ That is the same operator behaviour W29 identified in the Joomla extension cluster, now measured at global scale and directly applicable to the unmanaged South African web estate.

KPI Dashboard

Metric	Current (W30)	Prior (W29)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (10th week)	FLAT
ransomware.live SA cumulative	109	109	0	FLAT
New SA-linked leak-site claims	3	0	+3	UP
Confirmed SA incidents	2	0	+2	UP
Probable SA incidents (unconfirmed)	1	0	+1	UP
New CISA KEV additions	10	6	+4	UP
KEV adds rated CVSS 9.8 or above	4	6	-2	DOWN
Microsoft CVEs patched in window	621	0	+621	UP
Actively exploited MS zero-days	2	0	+2	UP
IR public statements in window	0	0	0	FLAT
Weeks since last IR publication	7	6	+1	UP

W30 KEY FRAMING: W30 is the week the domestic measurement caught up with the domestic reality. For six weeks this report has argued that zero new South African leak-site listings was a reporting artefact rather than an absence of attacks. This window delivered two confirmed incidents (BE Travel by ransomware, the Gauteng jobs portal by account compromise), a probable network breach at Rectron -- a top-four national technology distributor whose offices closed countrywide -- and two further leak-site claims. The common thread is supply chains: BE Travel books travel for the Housing Development Agency, Rectron supplies hardware and security products to a large share of the SA IT channel, and the Gauteng breach rode one ordinary user account against a control the Auditor-General had recommended and that remains unfunded two financial years later. Meanwhile external pressure rose on both axes at once -- ten KEV additions in seven days, the largest Microsoft release ever recorded, and an allied-agency alert confirming that the campaign against small unmanaged websites is global and industrial.

TOP 3 ACTIONS THIS WEEK

1. Clear the 17-19 July KEV deadlines, then treat CVE-2026-56164 as the exception to your severity threshold. Three deadlines have already passed as this report is read on 20 July: SonicWall SMA1000 CVE-2026-15409 and CVE-2026-15410 and SharePoint CVE-2026-56164 (17 July), Oracle E-Business Suite CVE-2026-46817 (18 July), and the two FortiSandbox flaws plus SharePoint CVE-2026-58644 (19 July). If any SonicWall SMA 1000 appliance was internet-reachable before 14 July, patching alone is insufficient -- these were exploited as zero-days, so assume pre-patch access and hunt accordingly. Confirm explicitly that CVE-2026-56164 was not skipped by a CVSS 7.0 or 8.0 patching gate.

2. Produce a written inventory of every internet-facing website your organisation owns, including the ones no one manages. The ACSC alert of 13 July names 17 CVEs across WordPress plugins (Ninja Forms, Gravity Forms, WPvivid Backup, Breeze Cache, GutenKit, Simple File List and others), Joomla JCE, Craft CMS, MaxSite and MetInfo, all of them public and patched, with webshell deployment as the objective and pivot into the corporate network as the follow-on. For each site record the CMS and plugin versions, the hosting party, and the named owner. Then check web directories for unexpected files in plugin folders and review access logs for GET or POST requests to unusual paths. Where a third party manages the site, send them the ACSC alert and require a dated written answer.

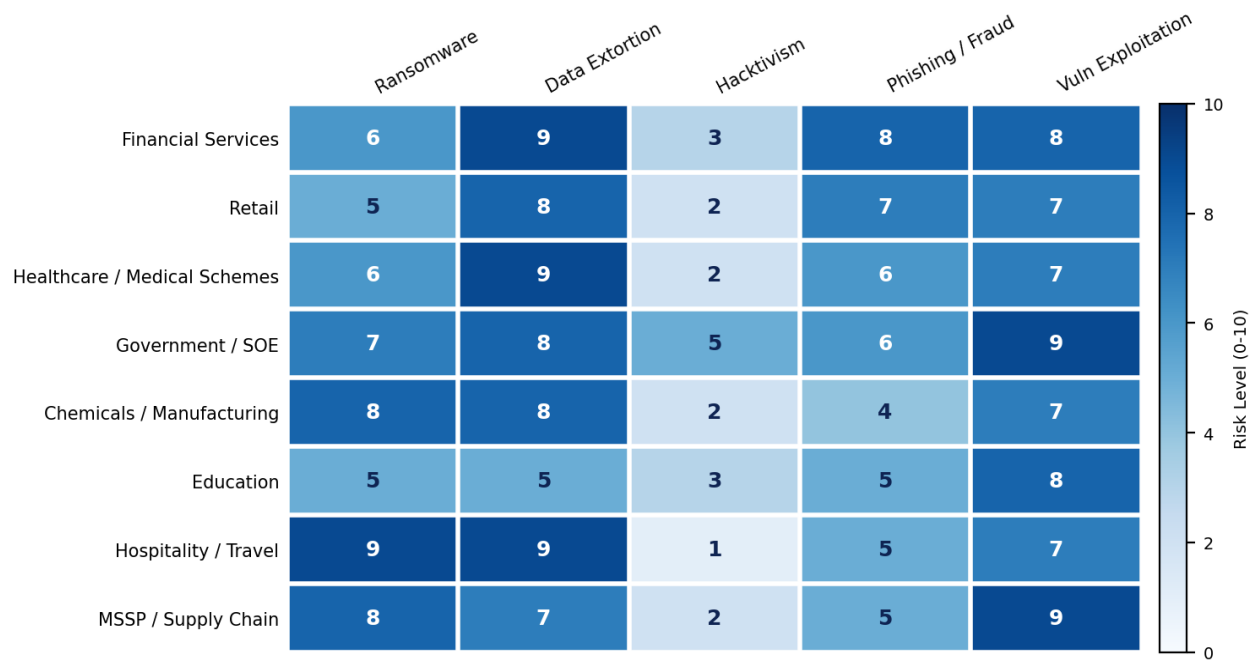
3. Audit AD FS and on-premises SharePoint as identity infrastructure, not as applications. CVE-2026-56155 is an exploited AD FS elevation-of-privilege flaw with a 28 July KEV deadline and, per ZDI, pairs with remote code execution in the combination commonly seen in ransomware intrusions. Patch it ahead of the deadline rather than on it, review AD FS administrative group membership and token-signing certificate history, and enumerate which SharePoint servers are reachable from the internet. On-premises SharePoint has now produced four separate KEV entries in three weeks.

1. Security Affairs -- Patch Tuesday security updates for July 2026, the largest update ever. 621 CVEs in one month (14 July 2026) -- <https://securityaffairs.com/195347/security/patch-tuesday-security-updates-for-july-2026-the-largest-update-ever-621-cves-in-one-month.html>
2. Security Affairs -- U.S. CISA adds SonicWall and Microsoft flaws to its Known Exploited Vulnerabilities catalog (15 July 2026) -- <https://securityaffairs.com/195383/security/u-s-cisa-adds-sonicwall-and-microsoft-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
3. Security Affairs -- U.S. CISA adds KNX Association KNX Protocol Connection Authorization Option 1 and Oracle flaws to its KEV catalog (17 July 2026) -- <https://securityaffairs.com/195516/security/u-s-cisa-adds-knx-association-knx-protocol-connection-authorization-option-1-and-oracle-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
4. Security Affairs -- U.S. CISA adds Fortinet FortiSandbox and Microsoft SharePoint flaws to its KEV catalog (18 July 2026) -- <https://securityaffairs.com/195569/security/u-s-cisa-adds-fortinet-fortisandbox-and-microsoft-sharepoint-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
5. Security Affairs -- U.S. CISA adds a Cisco IOS flaw to its Known Exploited Vulnerabilities catalog (13 July 2026) -- <https://securityaffairs.com/195262/security/u-s-cisa-adds-a-cisco-ios-flaw-to-its-known-exploited-vulnerabilities-catalog.html>
6. Security Affairs -- Australia Alerts Organizations to Ongoing CMS Exploitation Attacks (13 July 2026; ACSC alert, 17 CVEs) -- <https://securityaffairs.com/195208/security/australia-alerts-organizations-to-ongoing-cms-exploitation-attacks.html>
7. ITWeb -- Gauteng ignored AG warning before job portal breach (14 July 2026) -- <https://www.itweb.co.za/article/gauteng-ignored-ag-warning-before-job-portal-breach/Pero3MZ31O3qQb6m>
8. DeXpose -- DragonForce Targets South African Chemical Producer Isegen (18 July 2026; claim posted 15 July) -- <https://www.dexpose.io/dragonforce-targets-south-african-chemical-producer-isegen/>
9. Hendry Adrian -- Ransom: Be Travel, Arcus Media leak-site listing (July 2026; discovered 14 July) -- <https://www.hendryadrian.com/ransom-be-travel-jul-2026/>
10. Hendry Adrian -- Ransom: suppcentersa.com, m3rx leak-site listing (July 2026; posted 17 July) -- <https://www.hendryadrian.com/ransom-suppcentersa-com-jul-2026/>
16. MyBroadband -- South African company that books flights for agency in R29.6-billion government department hit by ransomware attack (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>

17. MyBroadband -- One of South Africa's largest technology distributors suffers crippling network outage allegedly due to cyberattack (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>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W30 (12 July - 19 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.

Hospitality / Travel is the week's sharpest movement, rising to 9 on both Ransomware and Data Extortion: BE Travel confirmed a 4 July ransomware incident, Arcus Media holds its data under a publication countdown, and the company services the Housing Development Agency's travel account -- a direct government supply-chain exposure.¹⁶ **Government / SOE** rises to 9 on Vulnerability Exploitation and 7 on Ransomware: the Gauteng e-Government jobs portal breach is CONFIRMED on the legislative record, and its stated cause -- a compromised non-privileged account against an unfunded, unimplemented Auditor-General control recommendation -- describes a structural condition across provincial and municipal IT rather than a single unlucky department; the HDA linkage of the BE Travel incident adds indirect exposure.⁷¹⁶ **MSSP / Supply Chain** rises to 8 on Ransomware on the probable Rectron breach: a top-four national technology distributor closing all offices nationwide is a channel-wide availability and integrity event whatever the final attribution.¹⁷ **Chemicals / Manufacturing** enters at 8 on Ransomware on the strength of the DragonForce claim against Isegen South Africa, a sector this report has not previously had cause to rate above baseline.⁸ **Vulnerability Exploitation** is elevated across every sector, reflecting ten KEV additions inside seven days and a 621-CVE Microsoft release; SonicWall SMA 1000 remote-access appliances and FortiSandbox concentrate in managed-service and mid-market estates.²⁴ **Financial Services** holds at 9 on Data Extortion on the still-unresolved Standard Bank / Liberty leak-site listing,

which remains indexed and unretracted.¹² **Hacktivism** is reduced to 5 for Government / SOE and 1-3 elsewhere: #OpSouthAfrica produced no observable activity for a third consecutive week, though exfiltrated Department of Correctional Services data remains in actor hands.

11. ITWeb -- SA records over 2 000 weekly cyber attacks (14 July 2026; Check Point Research June 2026 data) -- <https://www.itweb.co.za/article/sa-records-over-2-000-weekly-cyber-attacks/WnpNgM2ldgm7VrGd>

12. Ransomware.live -- South Africa country map and victim tracking (retrieved 19 July 2026; 109 cumulative) -- <https://www.ransomware.live/map/ZA>

3. TOP SA INCIDENTS (W30)

Week 30 (12 July - 19 July 2026) ends the six-week run of zero new South African leak-site listings, and does so across every confidence tier. Five items are recorded below: two CONFIRMED incidents (one acknowledged by the victim, one on the parliamentary record), one PROBABLE breach at a major technology distributor, and two leak-site claims of which one carries a disputed country attribution. The ransomware.live South African country-map total was 109 when retrieved on 19 July, unchanged from W29 -- the country map lags the individual group listings, which is itself a finding and is discussed in Section 6.¹² Each incident carries a confidence rating: CONFIRMED (victim or regulator acknowledgment, or two independent sources), PROBABLE (single credible source), CLAIMED (threat-actor assertion only).

3.1 INC-2026-W30-01 -- Gauteng Department of e-Government Jobs Portal Breach [CONFIRMED]

Sector	Government / Provincial administration (Gauteng Province)
Date	Disclosed 14 July 2026 via written reply to the Gauteng Provincial Legislature
Confirmed	283 application records from the provincial e-Recruitment (Jobs Portal) system: application forms, CVs, qualifications, certified copies of South African ID documents, contact details and proof of residence
Stated cause	Compromised non-privileged user account; department states this was not an infrastructure vulnerability and that MFA was enabled on all accounts
Control gap	Network Access Control system recommended by the Auditor-General in the 2023/24 audit was never implemented -- department cites lack of funding; no post-breach penetration test or additional audit was performed
Significance	Highest-sensitivity identity document set in a single small breach; job applicants are a population with limited ability to detect or respond to misuse of their identity documents
Confidence	CONFIRMED (executive acknowledgment on the legislative record)

Gauteng MEC for e-Government Bonginkosi Dhlamini confirmed the breach in a written reply to Democratic Alliance questions in the Gauteng Provincial Legislature, reported on 14 July.⁷ The record count is small at 283, but the field set is close to a worst case for identity fraud: a certified ID copy together with proof of residence and a full CV supplies most of what is needed to open accounts, port a SIM or pass a knowledge-based verification check. Job applicants also have no ongoing relationship with the department through which they would notice misuse. Two details deserve board attention beyond the incident itself. First, the department's own account is that MFA was enabled and a non-privileged

credential was still sufficient to reach 283 complete applicant files -- an authorisation and data-access design problem, not an authentication one. Second, the Auditor-General recommended a Network Access Control system in the 2023/24 audit and it remains unimplemented on funding grounds, which converts a known finding into an accepted risk without an accompanying compensating control. No post-breach penetration test was conducted. Affected applicants should be treated as at elevated risk of identity-document fraud and SIM-swap attempts through the remainder of 2026.

3.2 INC-2026-W30-02 -- DragonForce Claims Isegen South Africa (Pty) Ltd [CLAIMED]

Sector	Chemicals / Manufacturing (KwaZulu-Natal; isegen.co.za)
Date	Claim posted 15 July 2026; aggregator reporting 18 July 2026
Claimed	Data theft, with threat to publish the full dump absent negotiation
Corroboration	Single threat-intelligence aggregator; no victim statement, no sample data verified, no South African mainstream coverage located, not yet reflected on the ransomware.live country map
Actor	DragonForce -- ransomware-as-a-service operation with prior South African victims
Significance	First South African leak-site claim recorded by this report in seven weeks; extends targeting into industrial chemicals, a sector with OT adjacency
Confidence	CLAIMED (threat-actor assertion only, single aggregator source)

DragonForce listed Isegen South Africa on its leak site on 15 July, asserting that data had been stolen and threatening full publication unless negotiations began.⁸ No sample has been verified and Isegen has made no public statement, so this remains an uncorroborated actor claim and should not be reported internally as a confirmed breach. It is nonetheless the most significant leak-site development for South Africa since early June. Isegen produces itaconic acid and related speciality chemicals; a manufacturer of that profile typically runs an ERP estate alongside plant control systems, and DragonForce's established pattern is data theft with extortion rather than pure encryption, which means the OT environment is not necessarily implicated even if the claim is accurate. Organisations with Isegen in their supply chain should ask for a written status update rather than waiting for publication of the dump.

3.3 INC-2026-W30-03 -- BE Travel Ransomware Incident: Arcus Media, Housing Development Agency Contract [CONFIRMED]

Sector	Hospitality / Travel with government supply-chain reach (betravel.co.za, Baithaupi Executive Travel)
Date	Incident 4 July 2026; Arcus Media leak-site listing 13 July; victim confirmation reported 18 July
Confirmed	Ransomware incident on a dedicated server hosting the travel voucher and administration management system; full names, residential addresses and contact details of shuttle-service customers plus travel voucher data may have been accessed or encrypted; POPIA notifications issued to affected data subjects; Information Regulator obligations engaged; contact attempts from Arcus Media received but not engaged

Government link	Holds the active 36-month travel-management tender for the Housing Development Agency, the state property developer within the Department of Human Settlements (2026/27 budget R29.6 billion); the HDA did not comment by publication
Leak countdown	Arcus poster 'Fyodor Dostoevsky' announced publication of exfiltrated data seven days from 13 July -- expiry 20-21 July 2026, as this report is read
Confidence	CONFIRMED (information officer confirmation on the record, corroborating the 13 July leak-site listing)

BE Travel's information officer, Jerry Sekhwala, confirmed that the company suffered a ransomware incident on 4 July 2026, that the affected environment was isolated and taken offline immediately, that POPIA notifications have been issued to affected clients and stakeholders, and that the company is aware of attempted communications from Arcus Media but has not engaged with the actor.¹⁶ That converts last week's uncorroborated leak-site listing into the first victim-confirmed South African ransomware incident this report has recorded since May.⁹ Two features raise its significance beyond the company's size. First, the government supply chain: BE Travel holds the Housing Development Agency's active 36-month travel tender, meaning travel patterns and personal details of officials working on state housing projects may sit in the affected voucher system; the HDA did not comment by publication.¹⁶ Second, the timeline: nine days elapsed between the 4 July compromise and the 13 July leak-site listing, and the actor's seven-day countdown expires as this report is read -- the publication status must be re-checked on 20-21 July. Organisations that book travel through third-party agencies should establish in writing what personal data the agency holds on their employees and what its breach-notification obligation to them is.

3.4 INC-2026-W30-04 -- m3rx Claims SuppCenter Global Services [CLAIMED; SA attribution disputed]

Sector	MSSP / Managed security services (suppcentersa.com; Xcitium / Comodo partner)
Date	Leak-site post 17 July 2026
Claimed	Data theft; victim tagged country ZA on ransomware.live
Attribution caveat	The same record describes the company as a leading Xcitium partner in Latin America and lists a Costa Rican (+506) contact number; the 'sa' in the domain is more consistent with a regional abbreviation than with South Africa
Significance	Recorded to prevent an unreliable country tag propagating into automated South African feeds; the MSSP victim profile is relevant regardless of jurisdiction
Confidence	CLAIMED; South African attribution assessed as UNRELIABLE

m3rx listed suppcentersa.com on 17 July with a ZA country tag.¹⁰ This report does not count it as a South African victim: the same source record describes the organisation as an Xcitium partner operating in Latin America with a Costa Rican telephone number, making the ZA tag most likely a geolocation artefact. It is documented because the tag is machine-readable and will otherwise propagate into automated South African threat feeds as a phantom domestic incident. Treat single-source geographic attribution in leak-site data as an indicator requiring confirmation, not a fact.

3.5 INC-2026-W30-05 -- Rectron Nationwide Network Outage, Alleged Cyberattack [PROBABLE]

Sector	Technology Distribution / IT Supply Chain (one of SA's four largest distributors)
Date	Outage from 16 July 2026 (first notice 15:58); all offices closed 17 July; reported 19 July
Confirmed	Network outage acknowledged by Rectron in public notices; all offices closed nationwide -- Johannesburg (Midrand), Cape Town, Durban, Bloemfontein and Port Elizabeth; only the main Johannesburg line functional
Alleged	Sources close to the matter attribute the outage to a breach of the distributor's network; cybersecurity specialists dispatched to investigate; Rectron neither confirms nor denies a cyber incident
Significance	Channel-wide impact: Rectron distributes hardware and enterprise security products (Microsoft, Bitdefender, Acronis partnerships) to a large share of the SA IT reseller base; a multi-day nationwide closure is consistent with containment of a serious intrusion
Confidence	PROBABLE (outage CONFIRMED by the company; cyberattack attribution from a single credible source, not confirmed or denied by the victim)

Rectron first posted notice of a network outage on Thursday 16 July at 15:58, and by Friday 17 July had closed all of its offices nationwide while teams worked to restore operations.¹⁷ Sources close to the matter told MyBroadband the outage followed a breach of the distributor's network and that external cybersecurity specialists had been brought in; Rectron's formal statement neither confirmed nor denied a cyber incident, saying only that the issue was still being investigated.¹⁷ The outage itself is CONFIRMED; the cause is rated PROBABLE pending acknowledgment or disproof. The incident matters well beyond one company: Rectron is one of South Africa's four largest technology distributors and a significant channel for enterprise security products, so resellers and their end customers face order, licensing and support disruption, and -- if the breach attribution holds -- a potential supply-chain trust question over systems that integrate with the distributor's ordering and licensing platforms. Channel partners should monitor for a disclosure, treat unexpected 'Rectron' order or invoice correspondence with suspicion until the company clarifies the cause, and review any credentials or API integrations shared with the distributor. No ransomware group had claimed Rectron on any leak site checked by 19 July.

Carryover Status (checked 19 July 2026)

Profmed / PPS Healthcare Administrators: no scope expansion and no Information Regulator statement. KeyHealth, SEDMED, De Beers Benefit Society and the SANDF Regular Force Medical Continuation Fund remain neither confirmed nor excluded. This is now seven weeks unresolved and remains the highest-value unresolved South African exposure. **Standard Bank / Liberty (Prinz Eugen / ROOTBOY):** the ransomware.live listing is unchanged and unretracted; no new public development.¹² **AVBOB Mutual Assurance:** approximately seven weeks post-incident with no leak-site claim and no attribution; exposure remains UNDETERMINED. **Pick n Pay Asap!/Bottles and Capitec card replacements:** no development in the window. **#OpSouthAfrica (Nullsec Nigeria / Anonymous Nigeria):** no new leaks, defacements or claims for a third consecutive week; Department of Correctional Services data remains in actor hands and the campaign is unrenounced -- dormant, not resolved. Telegram and dark-web channels were not directly observable. **SAPS Western Cape POPIA breach:** no Information Regulator statement or investigation outcome.¹³ **Tembisa Hospital information-officer prosecution:** no prosecution decision published. **ICASA / Session Telecoms:** no published progress on the operator's review application and no regulator or MTN response to the industry-wide SIM-boxing allegation.

13. Information Regulator (South Africa) -- Media statements (checked 19 July 2026; most recent statement dated 2 June 2026) -- <https://info regulator.org.za/media-statements/>

4. THREAT ACTORS

4.1 DragonForce [CLAIMED activity against SA]

DragonForce is a ransomware-as-a-service operation running a data-theft-and-extortion model, and it is the actor behind the only new South African corporate leak-site claim of the window, against chemical producer Isegen South Africa on 15 July.⁸ The group's public messaging in this claim follows its standard template -- an assertion of theft, a demand that negotiations begin, and a threat of full publication -- with no proof pack published at the time of writing. DragonForce affiliates have previously been observed abusing signed but vulnerable Microsoft-ecosystem drivers to disable endpoint protection, a technique that shows up in telemetry as unexpected kernel driver loads shortly before mass file access. Assessment: an established operator with demonstrated South African targeting, currently the highest-priority ransomware actor for domestic manufacturing and industrial estates.

4.2 Arcus Media [CONFIRMED activity against SA]

Arcus Media is the confirmed actor behind the BE Travel incident: the victim acknowledged the 4 July compromise and attempted contact from the group, which listed the company on its leak site on 13 July under the poster persona 'Fyodor Dostoevsky' with a seven-day publication countdown.¹⁶⁹ The group's operators post under the names of Russian writers and philosophers, and its site carries the standard coercive framing ('each target has a chance to stay private'). It is prolific and indiscriminate, with hundreds of victims globally across education, healthcare, government suppliers and financial services, including Kenya's East African Gasoil in November 2025 -- an established African targeting footprint. Its selection of a mid-sized travel agency with a government contract is consistent with the broader 2026 pattern of extortion groups moving down-market to organisations that hold high-value personal data but lack a security function. Assessment: confirmed active against South Africa this window; the victim profile is more representative of typical South African exposure than the headline enterprise groups.

4.3 The Gentlemen [CONFIRMED research; prior SA victim]

Check Point Research data for June 2026, published in South Africa on 14 July, records The Gentlemen overtaking Qilin as the most active ransomware group globally, accounting for 17 percent of publicly reported attacks against Qilin's 11 percent, with LockBit rebuilding from 1 percent to 7 percent.¹¹ The Gentlemen already holds a South African victim on ransomware.live in food manufacturer Sunspray Food, listed in April 2026.¹² A group reaching the top of the global leaderboard while holding existing South African victims is a forward indicator worth tracking rather than a current incident. Assessment: elevated watch status for South African manufacturing and food production.

4.4 CMS Webshell Exploitation Cluster [CONFIRMED campaign; UNATTRIBUTED]

The Australian Signals Directorate's 13 July alert describes a large-scale global campaign exploiting known CMS vulnerabilities to deploy webshells: 17 CVEs across WordPress plugins (Ninja Forms, Gravity Forms, WPvivid Backup, Breeze Cache, GutenKit, Simple File List and others), Joomla JCE, Craft CMS, MaxSite and MetInfo.⁶ All are public and patched -- every successful compromise lands on an unpatched estate -- and the ACSC names small and medium businesses among the victims, linking the tempo to a Five Eyes

statement on AI shortening the disclosure-to-exploitation interval. Objectives run from credential capture to using the web server as a pathway into the corporate network. Assessment: the same tradecraft W29 identified in the Joomla extension cluster, now confirmed at global scale; highest-priority actor for South African web estates and the most likely source of the next domestic victim.

4.5 SonicWall SMA 1000 Zero-Day Operator [CONFIRMED exploitation; UNATTRIBUTED]

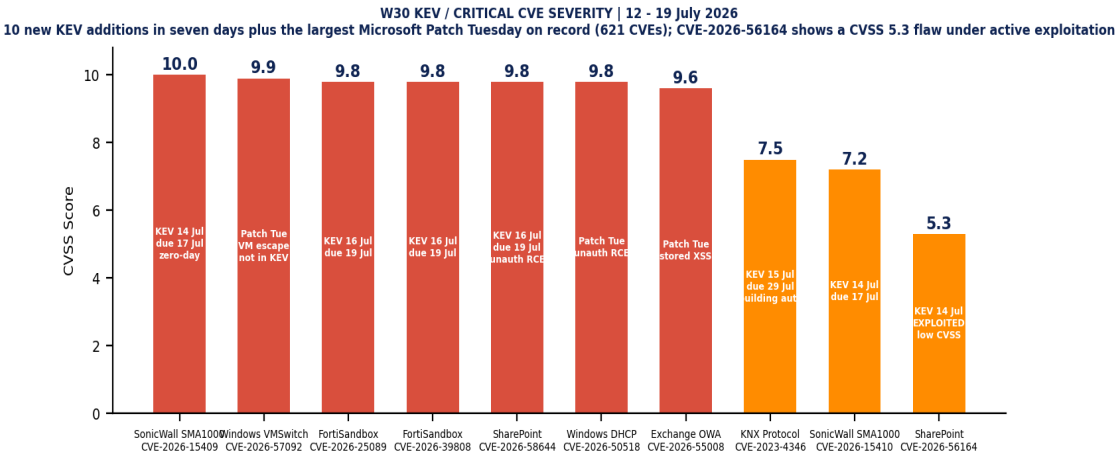
SonicWall confirmed active zero-day exploitation of two SMA 1000 flaws discovered by its own PSIRT: CVE-2026-15409 (CVSS 10.0, unauthenticated SSRF in the Work Place interface) and CVE-2026-15410 (CVSS 7.2, post-auth code injection in the management console executing OS commands as administrator).² Multiple exploitation cases were investigated; no actor named, no victim identified. Assessment: remote-access appliance exploitation with zero-day access is the classic precursor to ransomware deployment or espionage staging. Because exploitation preceded the patch, any SMA 1000 exposed before 14 July must be treated as potentially compromised -- patching is not closure.

11. ITWeb -- SA records over 2 000 weekly cyber attacks (14 July 2026; Check Point Research June 2026 data) -- <https://www.itweb.co.za/article/sa-records-over-2-000-weekly-cyber-attacks/WnpNgM2ldgm7VrGd>

5. CRITICAL VULNERABILITIES & CISA KEV

Ten vulnerabilities entered the CISA KEV catalogue between 13 and 16 July 2026, against six the previous week, on the now-standard three-day fuses (17, 18 and 19 July deadlines; AD FS runs to 28 July and KNX to 29 July).²³⁴⁵ Three structural observations stand out. First, Microsoft's 14 July Patch Tuesday was the largest single-month release in company history at 621 CVEs with 63 rated Critical.¹ Second, one of the two actively exploited Microsoft zero-days, SharePoint CVE-2026-56164, is rated only CVSS 5.3 -- a missing-authentication flaw exploitable without credentials or user interaction, which any severity-threshold patching policy would have deferred. Third, Oracle E-Business Suite CVE-2026-46817, tracked by this report as exploited-but-uncatalogued since W28, was added to the KEV on 15 July with an 18 July deadline, closing an 18-day gap between observed exploitation and catalogue listing.³

W30 KEV / Critical CVE Severity Overview -- 10 New KEV Adds 13-16 July Plus Patch Tuesday Criticals



W30 CISA KEV / Critical CVE Tracking (new adds 13-16 July plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-15409	SonicWall SMA 1000 Appliances	10.0	SSRF (unauth)	17 Jul	KEV 14 Jul. Exploited as zero-day; SonicWall PSIRT investigated multiple cases. Assume pre-patch compromise if exposed.
CVE-2026-15410	SonicWall SMA 1000 Appliances	7.2	Code injection	17 Jul	KEV 14 Jul. Post-auth, AMC console, arbitrary OS commands as administrator. Chains with the SSRF flaw.
CVE-2026-56155	Microsoft AD Federation Services	n/a	Priv escalation	28 Jul	KEV 14 Jul. Actively exploited zero-day. ZDI notes pairing with RCE in ransomware intrusions. Longest fuse of the batch.
CVE-2026-56164	Microsoft SharePoint Server	5.3	Missing auth	17 Jul	KEV 14 Jul. Actively exploited despite Moderate rating; unauth, no user interaction. Severity-gate blind spot.
CVE-2026-46817	Oracle E-Business Suite (Payments)	n/a	Improper privilege mgmt	18 Jul	KEV 15 Jul, day 18 after observed exploitation. Versions 12.2.3-12.2.15; unauth takeover over HTTP. Fixed in the May 2026 CPU.
CVE-2023-4346	KNX Association KNX Protocol	7.5	Account lockout	29 Jul	KEV 15 Jul. Building automation; attacker sets BCU key and locks legitimate users out. Availability impact.
CVE-2026-25089	Fortinet FortiSandbox	9.8	OS command injection	19 Jul	KEV 16 Jul. Unauth via crafted HTTP requests. Defused Cyber observed exploitation within a 24-hour window.
CVE-2026-39808	Fortinet FortiSandbox	9.8	OS command injection	19 Jul	KEV 16 Jul. Second FortiSandbox command-injection flaw; unauth code or command execution.

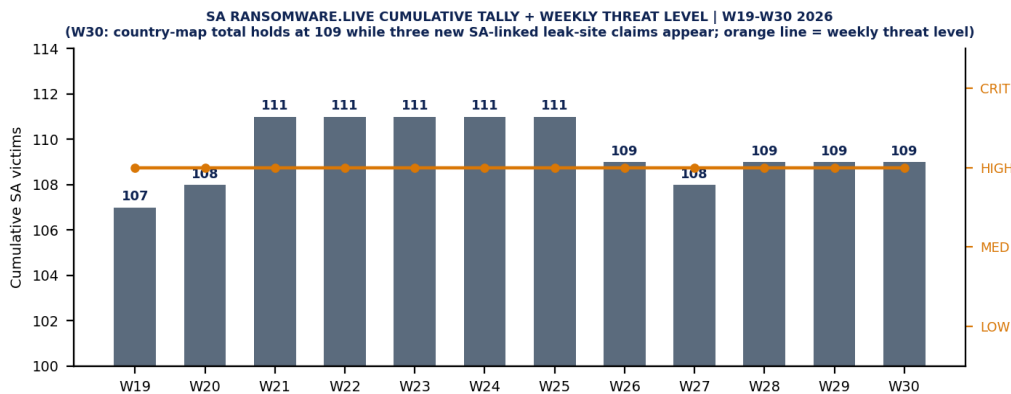
CVE-2026-58644	Microsoft SharePoint Server	9.8	Deserialization RCE	19 Jul	KEV 16 Jul. Fixed in the 14 July Patch Tuesday; Microsoft confirmed active exploitation. Fourth SharePoint KEV in three weeks.
CVE-2008-4128	Cisco IOS 12.4 / 871 ISR	n/a	CSRF	13 Jul	KEV 13 Jul, same-day deadline. An 18-year-old CVE in end-of-life hardware -- relevant to legacy SA branch estates.
CVE-2026-57092	Microsoft Windows VMSwitch	9.9	Use-after-free EoP	not in KEV	Patch Tuesday. Highest CVSS of the month. Guest VM to Hyper-V host escape. No KEV listing.
CVE-2026-50518	Microsoft Windows DHCP Server	9.8	Heap overflow RCE	not in KEV	Patch Tuesday. Unauthenticated and network-reachable. Prioritise any internet-facing DHCP.
CVE-2026-55008	Microsoft Exchange Server (OWA)	9.6	Stored XSS	not in KEV	Patch Tuesday. Listed as spoofing; ZDI advises treating as stored XSS in OWA executing on message view.
CVE-2026-45659	Microsoft SharePoint Server	8.8	Deserialization RCE	4 Jul	OVERDUE +16 days. KEV 1 Jul carryover. Verify remediation alongside CVE-2026-58644.

Pattern note: W30 inverts W29's signal. Last week the story was severity -- six additions, none below CVSS 9.8. This week severity stopped being a usable filter: the ten new KEV entries include an 18-year-old CSRF flaw in end-of-life Cisco hardware, an actively exploited flaw rated 5.3, and a building-automation availability flaw, while the highest-severity vulnerability of the month -- the CVSS 9.9 VMSwitch hypervisor escape -- has no KEV entry and therefore no deadline. Patching strictly by CVSS threshold misses the exploited SharePoint flaw; patching strictly by KEV membership misses the hypervisor escape. The workable rule is exposure-first: rank by whether the asset is internet-reachable and what it authenticates or hosts, then use KEV membership to set the clock and CVSS to break ties.

15. The Hacker News -- SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation (2 July 2026; carryover context) -- <https://thehackernews.com/2026/07/sharepoint-rce-cve-2026-45659-added-to.html>

6. RANSOMWARE LANDSCAPE

The ransomware.live South African country-map total was 109 when retrieved on 19 July 2026, unchanged from the 109 verified on 12 July.¹² Read alone, that would make W30 a seventh consecutive quiet week. It was the opposite. Inside the window: a victim-confirmed ransomware incident (BE Travel, compromised 4 July, listed by Arcus Media 13 July, confirmation reported 18 July),¹⁶ a leak-site claim against chemical producer Isegen South Africa by DragonForce on 15 July,⁸ a probable breach-driven outage at technology distributor Rectron from 16 July,¹⁷ and an SA-tagged m3rx claim this report rejects on attribution grounds.¹⁰ The gap between the flat country-map total and this activity is a data-quality finding in its own right, and the clearest evidence yet for a position this report has argued since W25: the ransomware.live country total is a lagging floor on South African ransomware activity, not a measurement of it. Aggregation lag means group-site postings take days to weeks to propagate into country roll-ups; attribution gaps mean victims without an obvious South African identity are never country-tagged at all; and incidents like Rectron's, with no leak-site claim, never enter the series in the first place. Practical implication: the country map is fit for trend-lines over quarters, not for answering whether South Africa was attacked this week. Transparency note: the country-map page returned relative timestamps consistent with a cached render, so the 109 figure is reported as retrieved rather than as a live count.



Baseline (W29)	109 cumulative SA victims, verified 12 July 2026
New SA leak-site claims	3 posted in window: Be Travel / Arcus Media (13 Jul; victim CONFIRMED 18 Jul), Isegen South Africa / DragonForce (15 Jul), suppcentersa.com / m3rx (17 Jul -- SA attribution rejected)
Off-leak-site incidents	Rectron nationwide outage from 16 Jul, breach attribution PROBABLE; no leak-site claim as of 19 Jul
Delistings / restorations	None observed
End count (W30)	109 on the ransomware.live country map, retrieved 19 July 2026 -- unchanged; new claims not yet reflected in the country roll-up
Counted as SA victims	2 of 3 claims assessed as genuinely South African (Isegen, Be Travel)
Global context (June 2026)	646 publicly reported ransomware victims worldwide, up 33 percent year on year; The Gentlemen 17 percent of published attacks, Qilin 11 percent, LockBit 7 percent (from 1 percent)

Threat-level drivers	Six-week domestic quiet ended; first confirmed SA public-sector breach in weeks; 10 KEV additions; record 621-CVE Microsoft release; ACSC global CMS campaign alert
----------------------	---

Group notes: DragonForce -- newly active against South Africa with the Isegen claim; data-theft extortion model, established RaaS operation (Section 4.1). **Arcus Media** -- BE Travel incident now victim-confirmed; the publication countdown expires 20-21 July as this report is read, so re-check status immediately. **The Gentlemen** -- now the most active group globally at 17 percent of published attacks per Check Point's June data, and already holds South African food manufacturer Sunspray Food from April 2026.¹¹¹² **Prinz Eugen / ROOTBOY** -- the Standard Bank / Liberty listing remains indexed and unretracted with no new movement.¹² **Qilin** -- displaced from the top position for the first time in the current series but still second globally at 11 percent, and historically active against African targets. **LockBit** -- share rose from 1 percent to 7 percent month on month, the clearest sign yet of rebuilding after prior law-enforcement disruption; treat any LockBit-branded activity against South African targets as a genuine re-emergence rather than an impersonator by default.

7. OSINT EXPOSURE & ATTACK SURFACE

Content management systems -- the unmeasured South African web estate

The ACSC alert of 13 July is the most operationally useful exposure finding of the week for South African organisations, because it converts an abstract risk into a finite checklist.⁶ Seventeen named CVEs across WordPress plugins, Joomla JCE, Craft CMS, MaxSite and MetInfo are under active mass exploitation for webshell deployment, all of them public and already patched. The South African relevance is structural rather than speculative: a large share of domestic SME, NGO, school and municipal web presence runs on shared hosting with WordPress or Joomla, maintained by a web agency under a design contract with no security scope, and does not appear on any asset register held by the organisation that owns the brand. The ACSC names small and medium businesses among the confirmed victims. The follow-on risk is not defacement but the pathway the alert describes explicitly -- credential capture from site users, malware distribution to legitimate visitors, and use of the compromised web server as a route into the corporate network. Recommended exposure action: enumerate owned domains and subdomains from public DNS and certificate-transparency data, resolve each to a hosting party, and record CMS and plugin versions. Most organisations doing this for the first time find sites they had forgotten they owned.

SonicWall SMA 1000 -- remote-access appliance exposure

CVE-2026-15409 (CVSS 10.0) is an unauthenticated SSRF flaw in the SMA 1000 Work Place interface, the component that is by design internet-facing, and it was exploited before a patch existed.² Exposure duration therefore matters more than patch status: any appliance reachable from the internet prior to 14 July should be treated as potentially accessed. SMA 1000 concentrates in South African mid-market and managed-service estates as a legacy VPN platform. Exposure action: identify SMA appliances by external scan, confirm firmware, review Work Place access logs from 1 July onward, and rotate credentials and session tokens issued through the appliance.

On-premises SharePoint and Oracle E-Business Suite

On-premises SharePoint has generated four KEV entries in three weeks -- CVE-2026-45659 (overdue since 4 July), CVE-2026-56164 and CVE-2026-58644 -- against continuing Storm-2603 / Warlock

ransomware activity; treat it as a standing high-exposure asset rather than patching reactively.¹⁵²⁴ Oracle EBS CVE-2026-46817 (Payments 12.2.3-12.2.15, unauthenticated takeover over HTTP) was fixed in the May 2026 CPU, so any instance still vulnerable on 18 July has been exposed for over two months; SA ERP estates in manufacturing, mining and retail are the relevant population.³ The next Oracle Critical Patch Update falls on 21 July 2026, the day after this report is published.

8. REGULATORY & POLICY

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

The Information Regulator's media-statements page, checked on 19 July 2026, carries nothing newer than the 2 June 2026 statement on enforcement notices issued for POPIA and PAIA contraventions by public and private bodies.¹³ The separate enforcement-notices page shows the most recent notice as the Gauteng Department of Health matter under section 77J of PAIA, dated 10 June 2026.¹⁴ That is seven weeks without a published media statement and six weeks without a published enforcement notice, in a period covering a confirmed provincial-government breach of identity documents. The absence of publication is not evidence of inactivity -- investigations and assessments are not published in progress -- but for regulated entities it removes the main signal through which enforcement posture is read. Practical consequence: South African organisations currently have no recent published precedent against which to calibrate their own breach-notification decisions, and should default to the conservative reading of section 22.

The Gauteng breach as a POPIA test case [CONFIRMED facts, PROBABLE implications]

Three regulatory features of the Gauteng disclosure deserve separation from the incident itself.⁷ Disclosure reached the public through a legislature reply rather than a regulator statement or departmental notification, raising the question of whether and when section 22 notification to the Regulator and the 283 data subjects occurred. The department's confirmation that a 2023/24 Auditor-General control recommendation remains unimplemented for funding reasons creates a dated public record of a known unremediated weakness preceding a breach -- the evidential pattern that supports a section 19 finding. And no post-breach penetration test was conducted. The transferable lesson for information officers: an unimplemented audit finding attributed to budget is contemporaneous evidence of known risk after a breach. Where a control cannot be funded, record the compensating control and residual-risk acceptance in writing at the time, not afterwards.

TransUnion SA / Experian SA: section 59 responses remain unresolved [CONFIRMED]

No Information Regulator publication addresses the outcome of the TransUnion SA and Experian SA matters. The Regulator's published record on the credit bureaux still ends with the 25 March 2022 statement initiating an assessment of TransUnion and the 27 October 2021 statement on the Experian compromise; no subsequent outcome, enforcement notice or closure appears on either the media statements or the enforcement notices page as of 19 July 2026.¹³¹⁴ The responses this report recorded as due in early July are now approximately two weeks overdue with no public outcome. Organisations that consume bureau data should keep pre-drafted customer-facing language ready and confirm their contractual breach-notification rights, as recommended in W28 and W29.

Attack-volume benchmark: South Africa fourth in Africa [CONFIRMED research]

Check Point Research data for June 2026, published in South Africa on 14 July, places South African organisations at an average of 2,065 attacks per organisation per week, fourth on the continent behind Angola (4,890), Nigeria (4,361) and Kenya (2,646); the Africa-wide average of 3,008 is down 9 percent year on year while the global average of 2,270 rose 17 percent.¹¹ South Africa sits below the African average but above the global one -- which argues against the common domestic assumption of exceptional targeting and supports a proportionate, control-led investment case. The same dataset records that 3.9 percent of corporate generative-AI prompts carried a high risk of sensitive data exposure, with 85 percent of AI-using organisations seeing high-risk prompt activity -- a data-governance exposure outside most South African POPIA compliance programmes.

14. Information Regulator (South Africa) -- Enforcement notices (checked 19 July 2026; most recent notice dated 10 June 2026) -- <https://inforegulator.org.za/enforcement-notice/>

9. WEEKLY THREAT HUNT & IOCs

Seven hunt missions are active for W30. Three P1 missions address the exploited zero-days with lapsed or immediate deadlines: SonicWall SMA 1000, the two actively exploited Microsoft flaws from the 14 July Patch Tuesday, and the FortiSandbox command-injection pair. Three P2 missions cover the ACSC-documented CMS webshell campaign, Oracle E-Business Suite exploitation, and IT-distributor supply-chain exposure following the Rectron outage. One P3 mission addresses South African identity-document fraud arising from the Gauteng jobs portal breach. Hyper-V estates should additionally confirm coverage of the VMSwitch CVE-2026-57092 patch (CVSS 9.9, no KEV deadline -- see Section 5). A machine-readable indicator export accompanies this report (iocs_w30.csv). Note that the majority of indicators this week are behavioural rather than atomic: no public IP or hash indicator sets were released for the SonicWall, FortiSandbox or SharePoint exploitation in the window, and hunts are constructed accordingly.

TH-2026-W30-01 -- SonicWall SMA 1000 Zero-Day Exploitation Hunt**P1 -- CRITICAL: CVSS 10.0 unauth SSRF; exploited pre-patch; KEV due 17 Jul (LAPSED)**

Hypothesis: An unauthenticated attacker exploited CVE-2026-15409 (Work Place SSRF) and chained CVE-2026-15410 (AMC code injection) to execute OS commands as administrator. Exploitation preceded the patch, so any appliance internet-reachable before 14 July 2026 may have been accessed pre-patch; patching does not evict an attacker who already established access.

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

IOCs: Behavioural. Outbound HTTP from the appliance to internal RFC1918 addresses or 169.254.169.254; unrecognised AMC administrator logins; new or modified administrator accounts; unexpected process execution on the appliance OS; 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, firewall egress logs, VPN authentication logs, DMZ NetFlow, IdP logs for accounts authenticating through the appliance.

Detection Guidance: Patch immediately -- the 17 July deadline has passed -- then treat as suspected compromise: review Work Place and AMC logs from 1 July onward, validate every administrator account, rotate all credentials and session tokens issued through the appliance, and restrict AMC to a management network. If logs do not reach 1 July, record the retention gap as a finding.

TH-2026-W30-02 -- Microsoft Exploited Zero-Days: AD FS and SharePoint Missing-Auth Hunt**P1 -- CRITICAL: two exploited zero-days; KEV due 17 Jul (LAPSED) and 28 Jul**

Hypothesis: CVE-2026-56164 permits unauthenticated interaction with a SharePoint function that should require authentication and is exploited despite a CVSS of only 5.3. CVE-2026-56155 permits privilege escalation in AD FS and, per ZDI, typically pairs with an RCE in the pattern seen in ransomware intrusions. Combined hypothesis: unauthenticated entry through SharePoint, then identity-infrastructure escalation through AD FS to federated cloud access.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1606.002 (Forge Web Credentials: SAML Tokens), T1550.001 (Application Access Token), T1505.003 (Web Shell).

IOCs: Behavioural. SharePoint endpoints returning success without a preceding authentication event; new .aspx or .ashx files under LAYOUTS or content web roots; w3wp.exe spawning cmd.exe or powershell.exe; AD FS token-signing certificate changes outside a change window; new AD FS administrative group members; SAML assertions with unusual lifetimes or relying parties; cloud authentication from a federated identity with no on-premises logon.

Data Sources: IIS and SharePoint ULS logs, AD FS admin and security event logs (1200, 1202, 411), EDR process-creation telemetry, Entra ID sign-in logs, file-integrity monitoring on SharePoint web roots.

Detection Guidance: Apply the July 2026 updates now: the SharePoint deadline lapsed 17 July, AD FS is due 28 July -- patch ahead of the deadline. Verify CVE-2026-56164 was not excluded by a CVSS threshold in patch policy; if it was, fix the policy as a finding. Hunt backwards to 14 July, audit AD FS group membership and certificate history, and enumerate internet-reachable SharePoint servers.

TH-2026-W30-03 -- Fortinet FortiSandbox Command Injection Hunt**P1 -- CRITICAL:** two flaws at CVSS 9.8; unauth RCE; KEV due 19 Jul; exploitation seen in 24h

Hypothesis: An unauthenticated attacker sends crafted HTTP requests to a FortiSandbox appliance to execute arbitrary OS commands via CVE-2026-25089 or CVE-2026-39808; Defused Cyber observed exploitation within 24 hours of disclosure. FortiSandbox sits inside the security stack and is trusted by surrounding controls -- compromise yields both a foothold and visibility into what the organisation is already inspecting.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1078 (Valid Accounts), T1562.001 (Impair Defenses).

IOCs: Behavioural. HTTP requests to management or API endpoints from unexpected sources; shell metacharacters in request parameters; outbound connections from the appliance to non-Fortinet destinations; unexplained verdict or policy changes; new administrative accounts; gaps in submission logs.

Data Sources: FortiSandbox system, event and API logs, upstream firewall logs, NetFlow, FortiAnalyzer or SIEM verdict records, configuration change history.

Detection Guidance: Patch per Fortinet advisory FG-IR-26-100 -- the 19 July deadline has passed. Confirm the management interface is not internet-reachable. Review logs from 10 July onward for anomalous requests and egress, and re-examine verdicts rendered during any suspected compromise window rather than assuming prior scanning results remain reliable.

TH-2026-W30-04 -- CMS Webshell Campaign Hunt (ACSC 17-CVE Alert)**P2 -- HIGH:** confirmed global mass campaign; SMEs impacted; 17 public CVEs

Hypothesis: Automated scanning identifies an unpatched CMS or plugin from the ACSC-named set -- Simple File List, WavePlayer, BerqWP, WPBookit, Ninja Forms, ThemeREX Addons, Breeze Cache, pay-uz, ACF Extended, Sneeit Framework, WPvivid Backup, Gravity Forms, GutenKit/Hunk Companion, Craft CMS, MaxSite CMS, MetInfo CMS or Joomla JCE -- and exploits unauthenticated file upload, RCE, SSRF or deserialisation to deploy a webshell. The webshell is then used for credential capture from site visitors, malware distribution, or pivot into the corporate network from the web server.

MITRE ATT&CK: T1595.002 (Active Scanning: Vulnerability Scanning), T1190 (Exploit Public-Facing Application), T1505.003 (Server Software Component: Web Shell), T1105 (Ingress Tool Transfer), T1078 (Valid Accounts), T1021 (Remote Services).

IOCs: Behavioural and file-based. Unexpected .php files in plugin, theme, upload or cache directories; PHP files with recent modification timestamps inconsistent with deployment history; GET or POST requests to unusual paths, particularly single-file endpoints under wp-content/uploads or Joomla components; POST requests with base64 or hex-encoded parameter bodies; web server process spawning shell child processes; new CMS administrator or Super User accounts; outbound connections from the web host to non-CDN destinations.

Data Sources: Web server access and error logs, filesystem inventory and integrity monitoring of web roots, CMS audit and user tables, hosting-provider logs, egress netflow from web hosting segments, external attack-surface scans.

Detection Guidance: Enumerate every internet-facing site the organisation owns and record CMS, plugin versions, hosting party and named owner. Patch or remove the named plugins and inspect web directories for unexpected files. If a webshell is found, do not simply delete it: trace the initial exploitation through logs, look for lateral movement and new accounts, and restore from a known-good backup. Configure web directories read-only where possible and block unnecessary connections from web servers to internal systems. Where a third party manages the site, send them the ACSC alert and require a dated written response.

**TH-2026-W30-05 -- Oracle E-Business Suite
CVE-2026-46817 Hunt****P2 -- HIGH: unauth takeover over HTTP;
KEV added day 18; due 18 Jul (LAPSED)**

Hypothesis: An unauthenticated attacker exploits an improper privilege management flaw in Oracle Payments (E-Business Suite 12.2.3 through 12.2.15) to take over the system over HTTP. The fix shipped in the May 2026 Critical Patch Update, so any instance still vulnerable on 18 July has been exposed for more than two months, and exploitation was observed publicly from early July -- roughly two weeks before the KEV listing created a deadline. Catalogue-driven patching programmes were structurally late on this one.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1078.001 (Valid Accounts: Default Accounts), T1213 (Data from Information Repositories), T1567 (Exfiltration Over Web Service), T1136 (Create Account).

IOCs: Behavioural. HTTP requests to Oracle Payments and iPayment servlet paths from unexpected sources; privileged actions with no corresponding authentication event; new or modified EBS accounts and responsibility assignments; large exports or outbound transfers from EBS tiers; access to banking and payment configuration tables outside business processes.

Data Sources: Oracle EBS application and concurrent-manager logs, HTTP Server access logs, database audit trails on payment and user tables, WAF logs, ERP-tier egress netflow.

Detection Guidance: Apply the May 2026 CPU if not already done -- the KEV deadline lapsed 18 July -- and plan the 21 July CPU now. Confirm no EBS instance is internet-reachable without a WAF. Hunt backwards to 1 July with attention to account creation and responsibility changes, since the flaw concerns privilege management rather than code execution.

**TH-2026-W30-06 -- IT Distributor Supply-Chain Exposure
Hunt (Rectron Outage)****P2 -- HIGH: top-4 SA distributor down
nationwide; breach alleged, not denied**

Hypothesis: If the Rectron outage reflects a network breach, as sources allege and the company has not denied, then reseller and end-customer integrations with the distributor -- ordering portals, licensing provisioning (Microsoft, Bitdefender, Acronis), B2B APIs, EDI links and shared credentials -- constitute a potential downstream attack path, and correspondence purporting to come from the distributor becomes a high-credibility phishing pretext during the disruption window.

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

IOCs: Behavioural. Unexpected password-reset, banking-detail-change or invoice emails purporting to come from Rectron during or after the outage window (16 July onward); logins to reseller portal accounts from unfamiliar sources; anomalous activity on API keys or service accounts shared with the distributor; licensing or provisioning changes not initiated by your own staff; lookalike domains registered against the distributor's 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: Until Rectron publishes a definitive cause: verify any payment-detail or ordering change through a known contact on an existing number, not details supplied in new correspondence. Inventory credentials, API keys and integrations shared with the distributor and rotate any that are stale or over-privileged. Finance teams should treat distributor-branded invoice or banking-change requests as high-risk pending clarification. If a breach is confirmed, expect the follow-on risk to arrive as fraud against the channel rather than as further intrusion at the distributor.

TH-2026-W30-07 -- SA Identity-Document Fraud
Following the Gauteng Portal Breach

P3 -- MEDIUM: 283 certified ID copies exposed; SA-specific downstream fraud

Hypothesis: The 283 records exposed in the Gauteng e-Government jobs portal breach include certified copies of South African identity documents, proof of residence and full CVs -- the combination required to pass knowledge-based verification, open credit accounts, or execute a SIM swap. Affected individuals are job applicants with no ongoing relationship with the department and therefore no natural notification or detection channel. Downstream fraud is expected to appear at banks, mobile network operators and credit providers rather than at the breached department, and will not be self-evidently linked to this breach.

MITRE ATT&CK: T1589 (Gather Victim Identity Information), T1586 (Compromise Accounts), T1656 (Impersonation), T1598 (Phishing for Information).

IOCs: Behavioural, SA-specific. Account-opening or credit applications supported by certified ID copies and proof of residence clustered around Gauteng provincial recruitment cycles; SIM-swap requests for numbers in Gauteng public-sector applicant populations; verification attempts where supplied address does not match bureau records; recruitment-themed phishing impersonating provincial departments.

Data Sources: Bank and credit-provider onboarding and KYC systems, MNO SIM-swap logs, credit bureau enquiry records, fraud case management systems, email gateway telemetry, SABRIC member fraud reporting.

Detection Guidance: Financial services and telecoms should apply heightened verification to document-based onboarding matching this profile through 2026, and should not treat a certified ID copy plus proof of residence as sufficient independent verification. Expect recruitment-themed phishing referencing the breach itself. Public-sector recruitment portals should audit which accounts can read complete applicant files and reduce that set: one compromised non-privileged account reached 283 complete records here, an authorisation design failure independent of the credential compromise.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Close the lapsed KEV deadlines in priority order, treating exposure duration as the ranking factor.** SonicWall SMA 1000 first, because exploitation preceded the patch and the appliance is by design internet-facing; then SharePoint CVE-2026-58644 and CVE-2026-56164; then the FortiSandbox pair; then Oracle E-Business Suite. For SonicWall specifically, patching is the start of the response, not the end -- rotate credentials and session tokens and review logs from 1 July.
- 2. Fix the patch-prioritisation policy, not just the patches.** CVE-2026-56164 is rated CVSS 5.3 and is being actively exploited; CVE-2026-57092 is rated 9.9 and has no KEV entry. If your policy is 'patch KEV within deadline, patch CVSS 9.0-plus within 30 days', both of these fall through it. Move to an exposure-first model: internet-reachable assets and identity infrastructure get the shortest clock regardless of score, with KEV membership setting deadlines and CVSS breaking ties.
- 3. Build the CMS asset register this week.** Enumerate owned domains and subdomains from public DNS and certificate-transparency logs, resolve each to a hosting party and a named internal owner, and record CMS and plugin versions against the 17 CVEs in the ACSC alert. Then inspect web directories for unexpected files and review access logs for requests to unusual paths. This is the single highest-yield exercise available to a South African SOC this week.

4. Extend log retention to the assets in this report. Several hunts require logs back to 1 July; SonicWall appliance logs and Oracle EBS audit trails are commonly not collected or kept under 30 days. Where a hunt cannot run for want of data, record that as a finding on the risk register rather than closing the hunt as negative.

5. Treat AD FS and on-premises SharePoint as tier-zero identity infrastructure. Four SharePoint KEV entries in three weeks and an exploited AD FS privilege-escalation flaw justify a standing control set: restricted administrative group membership, token-signing certificate change alerting, internet-exposure review, and web-root file-integrity monitoring.

Management (CISO / Board)

1. The Gauteng breach is the governance lesson of the week and it is not about government. A control recommended by the auditor in 2023/24 went unimplemented for funding reasons, and the resulting breach produced a dated public record of a known unremediated weakness. Ask your own organisation one question: which audit or assessment findings are currently open on funding grounds, and for each, is the compensating control and residual-risk acceptance documented in writing and dated? An unfunded finding with no recorded compensating control is an accepted risk that nobody formally accepted.

2. Third-party data custody is now appearing in a new sector every month. Medical scheme administrators, retail delivery platforms, and this week a corporate travel agency holding passport scans and lodged card details for client organisations. Identify every third party that holds personal data on your employees or customers, and confirm in writing what they hold and what their breach-notification obligation to you is. Most organisations discover the obligation is unspecified.

3. Calibrate the attack-volume narrative honestly. Check Point's June data places South Africa fourth in Africa at 2,065 weekly attacks per organisation, below the African average and above the global one. That is a materially different story from the exceptional-targeting framing common in domestic discussion, and it supports a proportionate, control-led investment case rather than a crisis-led one.

4. Register the regulatory silence as a planning assumption. The Information Regulator has published nothing for seven weeks and the credit-bureau matters remain without published outcome. Do not read absence of enforcement as tolerance; plan on the conservative reading of section 22 notification.

5. Put generative AI data exposure on the risk register. Check Point's data records 3.9 percent of corporate AI prompts carrying high risk of sensitive data exposure. Most South African POPIA programmes do not treat prompt content as a processing activity; that gap will close by incident or by regulation, and closing it deliberately is cheaper.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH -- 10th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for a tenth consecutive week (12 July - 19 July 2026). Unlike the preceding six weeks, the level no longer rests primarily on external exploitation tempo with an inferred domestic exposure. This week the domestic evidence arrived at every confidence tier: a victim-confirmed ransomware incident with a government supply-chain dimension (BE Travel / Housing Development Agency), a confirmed provincial-government breach of identity documents (Gauteng), a probable breach-driven nationwide shutdown at a top-four technology distributor (Rectron), and leak-site claims against a chemical producer. The case for escalation to CRITICAL was considered and narrowly rejected: the confirmed incidents are contained in scale, the Rectron cause is not yet acknowledged, and no systemically important institution is confirmed compromised. If the Rectron breach is confirmed with channel impact, or the BE Travel data publishes with material HDA content, that calculus changes. The case for de-escalation no longer exists.

Rationale

- **The domestic quiet ended at every confidence tier:** BE Travel CONFIRMED by the victim (ransomware, 4 July, Arcus Media, POPIA notifications issued); Rectron PROBABLE (nationwide closure, breach alleged, not denied); Isegen / DragonForce and the rejected m3rx tag CLAIMED -- after six weeks of zero new listings.
- **Government supply-chain exposure is live:** BE Travel holds the Housing Development Agency's active 36-month travel tender, so a state entity's travel and personnel data sits inside a breached SME's voucher system, with the actor's publication countdown expiring 20-21 July.
- **A confirmed public-sector breach of identity documents:** 283 Gauteng jobs portal records including certified ID copies, proof of residence and CVs, caused by one compromised non-privileged account against an unfunded, unimplemented Auditor-General control recommendation -- a structural condition, not an isolated failure.
- **KEV volume rose 67 percent:** ten additions in seven days against six the prior week, with 17, 18 and 19 July deadlines that have all lapsed by publication, and three exploited zero-days among them.
- **Severity has stopped functioning as a filter:** an actively exploited SharePoint flaw rated CVSS 5.3 sits alongside a CVSS 9.9 hypervisor escape with no KEV entry and therefore no deadline. Both common patching policies fail on one of the two.
- **The largest Microsoft release ever recorded:** 621 CVEs on 14 July, 63 Critical, two under active exploitation, with the 2026 year-to-date count already exceeding every full-year total of the last two decades -- a change-management load most South African estates cannot absorb in a single cycle.
- **An allied agency confirmed the web-estate campaign at global scale:** the ACSC alert names 17 CVEs across WordPress, Joomla, Craft, MaxSite and MetInfo with SMEs explicitly among the victims, validating the Joomla-cluster assessment made in W29 and widening it to the whole unmanaged

South African web estate.

- **Carryovers remain unresolved, not retired:** Profmed / PPSHA scope (four schemes unconfirmed, including the SANDF RFMCF) at seven weeks, AVBOB undetermined at seven weeks, the Standard Bank listing unretracted, TransUnion and Experian responses approximately two weeks overdue with no published outcome, and #OpSouthAfrica dormant with DCS data still held.
- **Regulatory signal remains absent:** the Information Regulator has published no media statement since 2 June and no enforcement notice since 10 June, across a window containing a confirmed provincial-government breach.

Next-Week Watch (W31)

- **BE Travel countdown, 20-21 July:** whether Arcus Media publishes the exfiltrated dataset, whether Housing Development Agency or Department of Human Settlements data appears in it, and any HDA statement -- the agency did not comment by publication.
- **Rectron:** whether the company confirms or denies a cyberattack as the cause of the nationwide outage, any leak-site claim, service-restoration timeline, and any channel-facing fraud exploiting the disruption.
- **Isegen South Africa:** any victim statement, proof-pack publication, or appearance of the listing on the ransomware.live country map -- and whether the SA country total finally moves off 109.
- **Oracle Critical Patch Update, 21 July:** volume, any new E-Business Suite items, and whether CVE-2026-46817 exploitation reporting names victims.
- **AD FS CVE-2026-56155 deadline, 28 July:** whether exploitation expands and a paired RCE emerges, as ZDI anticipates.
- **First named South African victim of the CMS webshell campaign:** most plausibly a municipality, school, NGO or SME on shared hosting; watch for further CMS or plugin KEV additions.
- **SonicWall SMA 1000:** post-deadline exploitation reporting, victim identification, and any actor attribution for the zero-day operator.
- **Information Regulator:** any publication at all after seven weeks, particularly on the Gauteng e-Government breach, TransUnion SA and Experian SA, or the SAPS Western Cape matter.
- **Profmed / PPSHA:** confirmation or exclusion of the four remaining administered schemes, especially the SANDF Regular Force Medical Continuation Fund.
- **Windows VMSwitch CVE-2026-57092:** whether exploitation is observed and whether CISA adds it to the KEV.
- **FIC:** the 31 July second-batch RCR deadline and any first cross-border cash conveyance enforcement statement.

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 1-17 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 19 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 2, 3, 4 and 5). The two cited MyBroadband articles (items 16 and 17) were successfully retrieved in full on 19 July 2026 and verified directly, despite that domain having blocked retrieval in prior editions. The ransomware.live country map (item 12) returned a cached render; the 109 figure is reported as retrieved, not as a guaranteed live count (Section 6).

1. Security Affairs -- Patch Tuesday security updates for July 2026, the largest update ever. 621 CVEs in one month (14 July 2026) -- <https://securityaffairs.com/195347/security/patch-tuesday-security-updates-for-july-2026-the-largest-update-ever-621-cve-in-one-month.html>
2. Security Affairs -- U.S. CISA adds SonicWall and Microsoft flaws to its Known Exploited Vulnerabilities catalog (15 July 2026) -- <https://securityaffairs.com/195383/security/u-s-cisa-adds-sonicwall-and-microsoft-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
3. Security Affairs -- U.S. CISA adds KNX Association KNX Protocol Connection Authorization Option 1 and Oracle flaws to its KEV catalog (17 July 2026) -- <https://securityaffairs.com/195516/security/u-s-cisa-adds-knx-association-knx-protocol-connection-authorization-option-1-and-oracle-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
4. Security Affairs -- U.S. CISA adds Fortinet FortiSandbox and Microsoft SharePoint flaws to its KEV catalog (18 July 2026) -- <https://securityaffairs.com/195569/security/u-s-cisa-adds-fortinet-fortisandbox-and-microsoft-sharepoint-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
5. Security Affairs -- U.S. CISA adds a Cisco IOS flaw to its Known Exploited Vulnerabilities catalog (13 July 2026) -- <https://securityaffairs.com/195262/security/u-s-cisa-adds-a-cisco-ios-flaw-to-its-known-exploited-vulnerabilities-catalog.html>
6. Security Affairs -- Australia Alerts Organizations to Ongoing CMS Exploitation Attacks (13 July 2026; ACSC alert, 17 CVEs) -- <https://securityaffairs.com/195208/security/australia-alerts-organizations-to-ongoing-cms-exploitation-attacks.html>
7. ITWeb -- Gauteng ignored AG warning before job portal breach (14 July 2026) -- <https://www.itweb.co.za/article/gauteng-ignored-ag-warning-before-job-portal-breach/Pero3MZ31O3qQb6m>
8. DeXpose -- DragonForce Targets South African Chemical Producer Isegen (18 July 2026; claim posted 15 July) -- <https://www.dexpose.io/dragonforce-targets-south-african-chemical-producer-isegen/>
9. Hendry Adrian -- Ransom: Be Travel, Arcus Media leak-site listing (July 2026; discovered 14 July) -- <https://www.hendryadrian.com/ransom-be-travel-jul-2026/>
10. Hendry Adrian -- Ransom: suppcentersa.com, m3rx leak-site listing (July 2026; posted 17 July) -- <https://www.hendryadrian.com/ransom-suppcentersa-com-jul-2026/>
11. ITWeb -- SA records over 2 000 weekly cyber attacks (14 July 2026; Check Point Research June 2026 data) -- <https://www.itweb.co.za/article/sa-records-over-2-000-weekly-cyber-attacks/WnpNgM21dgm7VrGd>
12. Ransomware.live -- South Africa country map and victim tracking (retrieved 19 July 2026; 109 cumulative) -- <https://www.ransomware.live/map/ZA>
13. Information Regulator (South Africa) -- Media statements (checked 19 July 2026; most recent statement dated 2 June 2026) -- <https://inforegulator.org.za/media-statements/>
14. Information Regulator (South Africa) -- Enforcement notices (checked 19 July 2026; most recent notice dated 10 June 2026) -- <https://inforegulator.org.za/enforcement-notice/>
15. The Hacker News -- SharePoint RCE CVE-2026-45659 Added to CISA KEV After Active Exploitation (2 July 2026; carryover context) -- <https://thehackernews.com/2026/07/sharepoint-rce-cve-2026-45659-added-to.html>
16. MyBroadband -- South African company that books flights for agency in R29.6-billion government department hit by ransomware attack (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>
17. MyBroadband -- One of South Africa's largest technology distributors suffers crippling network outage allegedly due to cyberattack (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-W30 | Published Monday 20 July 2026