



SOUTH AFRICA

CYBER THREAT INTELLIGENCE REPORT

Weekly OSINT Brief, Week 32 | 26 July – 2 August 2026

THREAT LEVEL: HIGH

TLP:WHITE

Report ID: SA-CTI-2026-W32 | Classification: TLP:WHITE

Published Monday 3 August 2026

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

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

TABLE OF CONTENTS

- 1. Executive Summary & KPI Dashboard**
- 2. Threat Landscape Heatmap**
- 3. Top SA Incidents (W32)**
- 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, 12th consecutive week (26 July - 2 August 2026)

Story 1. Four South African ransomware victims this report has never covered became visible at once, headed by Fidelity Services Group. The ransomware.live South African country map, retrieved on 2 August 2026, now stands at 116 cumulative victims and itemises four mid-July South African listings that were not visible when this report checked the same source a week earlier: Fidelity Services Group, claimed by RansomHouse on 15 July with an estimated attack date of 12 July; SuppCenter Global Services, claimed by M3rx on 17 July; Reatile Group, claimed by IncRansom on 18 July; and CKR Consulting Engineers, claimed by Payload on 19 July.¹²³ The most significant of the four is Fidelity Services Group, Southern Africa's largest integrated security solutions provider, running guarding, cash-in-transit and fire services across roughly 142 points of presence. None of the four organisations has issued a public statement, so all four are rated CLAIMED. The timing carries as much weight as the names. The aggregator lag in the country feed is now demonstrably running at two to three weeks, so a South African organisation can sit on a leak site for a fortnight before it appears in the country feed that most local teams watch.

Story 2. SARS issued a formal alert that criminals are now using generative AI to write its phishing emails, at the peak of filing season. On 28 July 2026 the South African Revenue Service published a scam alert describing an SMS and email wave telling recipients they are owed a refund, in one specimen R48 900, and directing them to a fraudulent site.⁴ The line that matters is the revenue service's own: 'SARS is noting with concern that the scammers are now using AI to generate professional-looking email templates that are harder to identify as fraudulent.'⁴ Eyewitness News carried the warning on 30 July.⁵ This is the first time in this series that a South African public body has formally named generative AI as the reason its brand-impersonation fraud has become harder to spot, and it lands while millions of taxpayers are actively expecting SARS correspondence. The practical consequence is that the single most widely taught consumer defence in South Africa, namely looking for bad spelling and clumsy grammar, has stopped working.

Story 3. Three new KEV additions, two of them already past their remediation date on the day this report is read. CISA added three vulnerabilities to the KEV catalogue in the window: Arista VeloCloud Orchestrator On-Prem CVE-2026-16812 (CVSS 10.0, OS command injection, vendor-confirmed zero-day) and Fortinet FortiOS CVE-2025-68686 on 27 July, and Cisco Secure Firewall Management Center CVE-2026-20316 (hard-coded credential) on 29 July.⁶⁷⁸ The Arista deadline was 30 July and the Cisco deadline 1 August, so both had lapsed before publication.⁹ Separately, an unpatched Fastjson 1.x remote code execution flaw (CVE-2026-16723, CVSS 9.0) is being exploited in the wild with no fix and no KEV listing,¹⁰ and Rapid7 published a working proof-of-concept for the already-exploited Check Point SmartConsole flaw on 29 July.¹¹ All three new KEV entries are network-edge or security-management products, the same category that vendor research this week identified as the ransomware ecosystem's preferred front door.¹²

KPI Dashboard

Metric	Current (W32)	Prior (W31)	Change	Direction
Overall SA threat level	HIGH	HIGH	No change (12th week)	FLAT
ransomware.live SA cumulative	116	115	+1	UP
SA leak-site claims newly surfaced	4	n/a (metric added W32)	new metric	FLAT
SA claims dated inside the window	0	1	-1	DOWN
Confirmed SA incidents	1 (SARS scam wave)	1	0	FLAT
New CISA KEV additions	3	6	-3	DOWN
KEV adds already overdue at publication	2	2	0	FLAT
Overdue KEV carryovers tracked	4	2	+2	UP
IR public statements in window	0	0	0	FLAT
Weeks since last IR publication	9	8	+1	UP

W32 KEY FRAMING: W32 is a visibility week. Nothing new was posted against a South African target between 26 July and 2 August, yet the domestic picture worsened, because four mid-July victims this report had no sight of surfaced at once, including the largest security services company in Southern Africa. This is what the reporting lag costs in practice: leak-site monitoring gives South African defenders a two-to-three-week-old view, so a quiet week is a statement about the feed. Treat any week's SA count as a floor that will later be revised upward. Externally, the week turns on timing. Three KEV additions is the lowest count since W28, but two of the three were already past their remediation date before this report reached a reader, and all three are edge or management-plane products. Add an exploited Fastjson flaw with no patch at all and a fresh public exploit for the Check Point management-plane bug, and the perimeter and the security management console remain where the pressure sits. Domestically, the SARS alert is the item to action this week, because it reaches every employee, not only a server estate.

TOP 3 ACTIONS THIS WEEK

1. Send a SARS-specific warning to every employee in the week of 3 August, and change the advice you give them. SARS confirmed on 28 July that refund-themed phishing is now AI-generated, with correct grammar, genuine branding and real employee names. Tell staff the old spot-the-typo test is dead: the only safe action is to log in at the official eFiling address typed by hand, never through a link, and to treat any refund figure quoted in an email or SMS as unverified. Forward specimens to phishing@sars.gov.za. Pair this with a technical control: block newly registered lookalike domains containing 'sars' or 'efiling' at the web proxy, and alert on inbound mail spoofing the sars.gov.za display name.

2. Patch the two lapsed KEV items on Monday 3 August, and treat the Arista VeloCloud flaw as a suspected compromise. Arista VeloCloud Orchestrator On-Prem CVE-2026-16812 (CVSS 10.0) is a vendor-confirmed zero-day whose KEV deadline was 30 July; Arista published three attacker IPs (8.19.75.217, 206.72.242.124, 206.72.242.162) that should be blocked and retro-hunted in netflow. Cisco Secure FMC CVE-2026-20316 (KEV deadline 1 August) is a hard-coded credential. Run 'cat /var/log/messages | grep license' in expert mode and treat references to /var/tmp/license.tmp as possible compromise, then rotate all credentials, keys and certificates on the appliance as Cisco advises. Apply the fixed VCO builds (5.2.3.14, 6.1.3.4, 6.4.2.4, 7.0.0.1 or later).

3. Run a targeted supplier check against the four newly surfaced ransomware listings, especially Fidelity Services Group. Fidelity Services Group (guarding, cash-in-transit, fire), Reatile Group (energy investments), CKR Consulting Engineers and SuppCenter Global Services were all claimed in mid-July and none has made a public statement. If any of them is your supplier, contractor or guarding provider, ask in writing what personal data they hold on your staff. Access-control records, ID copies, biometric enrolments and site rosters are the typical holdings for a physical-security provider, and they are the reason a guarding-company breach becomes a physical-security problem as well as a POPIA one. Do not wait for an announcement that may never come.

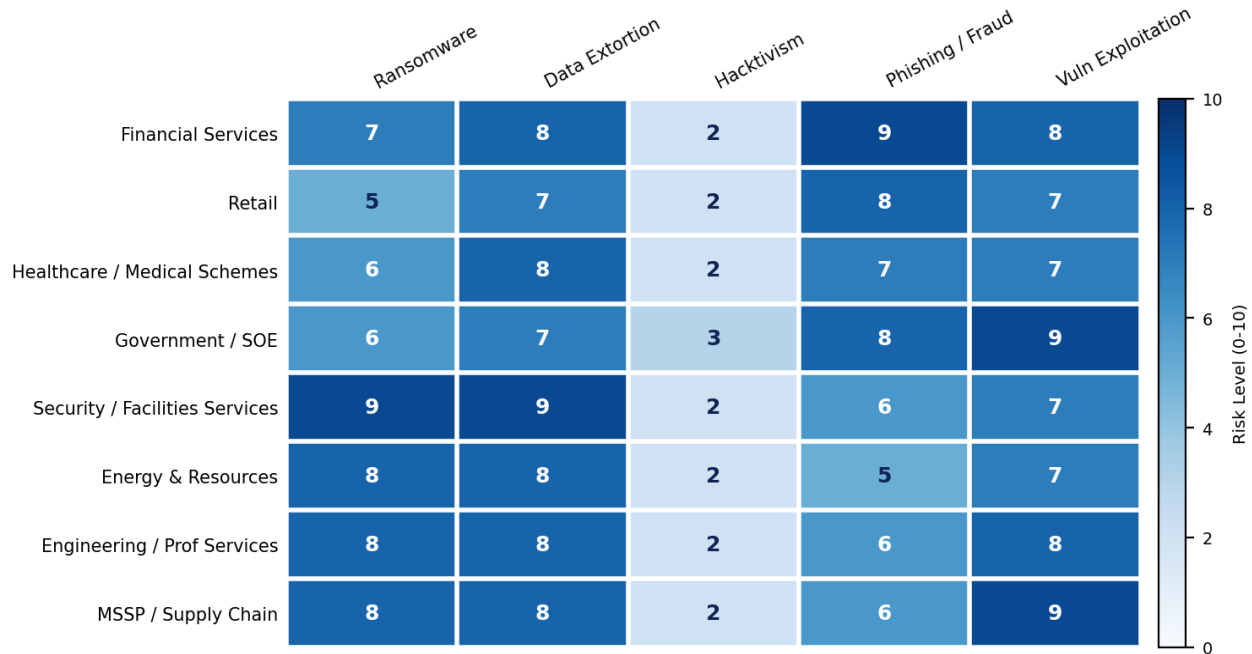
1. Ransomware.live, South Africa victim map: 116 cumulative victims (retrieved 2 August 2026). <https://www.ransomware.live/map/ZA>
2. Ransomware.live, Victim record: Fidelity Services Group / RansomHouse (discovered 15 July 2026; duplicate-entry flag; HudsonRock info-stealer data). <https://ransomware.live/id/RmlkZWxpdHkgU2VydmljZXMGd3JvdXBAdmFuc29taG91c2U>
3. DeXpose, IncRansom strikes South African energy-sector holding company Reatile Group (19 July 2026; claim posted 18 July). <https://www.dexpose.io/incransom-strikes-south-african-energy-leader-reatile-group/>
4. SARS, Scam alert: 'Tax Return Notification'; scammers now using AI to generate phishing templates (28 July 2026). <https://www.sars.gov.za/latest-news/scam-alert-tax-return-notification/>
5. Eyewitness News, SARS warns AI scams are targeting taxpayers (30 July 2026). <https://www.ewn.co.za/2026/07/30/sars-warns-ai-scams-are-targeting-taxpayers>
6. Security Affairs, U.S. CISA adds Arista VeloCloud Orchestrator and Fortinet FortiOS flaws to its Known Exploited Vulnerabilities catalog (28 July 2026). <https://securityaffairs.com/196130/security/u-s-cisa-adds-arista-velocloud-orchestrator-and-fortinet-fortios-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
7. The Hacker News, Attackers exploit Arista VeloCloud Orchestrator zero-day; FortiOS SSL-VPN patch-bypass added to KEV (28 July 2026). <https://thehackernews.com/2026/07/attackers-exploit-arista-velocloud.html>
8. Security Affairs, U.S. CISA adds a Cisco Secure Firewall Management Center flaw to its Known Exploited Vulnerabilities catalog (30 July 2026). <https://securityaffairs.com/196289/security/u-s-cisa-adds-a-cisco-secure-firewall-management-center-fmc-flaw-to-its-known-exploited-vulnerabilities-catalog.html>
9. Senserva, Exploited This Week: CISA KEV weekly summary and per-CVE due dates (updated 1 August 2026). <https://serva.com/exploited-this-week.html>
10. SecurityWeek, Unpatched Fastjson vulnerability exploited in attacks (28 July 2026). <https://www.securityweek.com/unpatched-fastjson-vulnerability-exploited-in-attacks/>

11. The Hacker News, Rapid7 releases proof-of-concept for exploited Check Point SmartConsole flaw (29 July 2026). <https://thehackernews.com/2026/07/rapid7-releases-poc-for-exploited-check.html>

12. Cyber Security News, Ransomware gangs attack Palo Alto, Fortinet, Citrix and Check Point VPNs to target corporate networks (27 July 2026). <https://cybersecuritynews.com/ransomware-gangs-attack-vpn/>

2. THREAT LANDSCAPE HEATMAP

SA THREAT LANDSCAPE HEATMAP | W32 (26 July - 2 August 2026)



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

Three rows change this week. **Security / Facilities Services**, **Energy & Resources** and **Engineering / Professional Services** replace Chemicals / Manufacturing, Education and Hospitality / Travel, following where this week's claims landed. The retired rows carry the still-open Isegen and BE Travel exposures, which are tracked in Section 3. Security / Facilities Services enters at 9 on Ransomware and 9 on Data Extortion. The driver is the RansomHouse claim against Fidelity Services Group, Southern Africa's largest integrated security provider.² A guarding and cash-in-transit business holds access-control logs, site rosters, ID copies and often biometric enrolments for the client sites it protects, so a compromise there is simultaneously a personal-information breach and a physical-security intelligence leak. **Energy & Resources** and **Engineering / Professional Services** both enter at 8/8 on the IncRansom claim against Reatile Group and the Payload claim against CKR Consulting Engineers respectively.³¹ **Financial Services** rises to 9 on Phishing / Fraud from 8 last week, the single highest cell in that column, on the strength of the SARS AI-generated refund campaign, which is a financial-fraud funnel even though the impersonated brand is a revenue authority.⁴ **Government / SOE** retains 9 on Vulnerability Exploitation given the unremediated edge-appliance estate implied by three consecutive weeks of network-perimeter KEV additions. **Hacktivism** stays uniformly low at 2-3: no South African hacktivist activity was observed in the

window and #OpSouthAfrica remains dormant.

3. TOP SA INCIDENTS (W32)

Week 32 (26 July - 2 August 2026) recorded no new South African leak-site claim dated inside the window. It did, however, make visible four mid-July claims that were not retrievable a week earlier, and it produced one confirmed nationwide fraud campaign carrying an official government warning. Incidents 3.1 to 3.4 are the newly surfaced listings, presented in order of assessed significance; 3.5 is the SARS campaign. All four leak-site items are rated CLAIMED: each rests on a threat-actor posting indexed by ransomware.live or DeXpose, none has a victim statement, and this report does not treat an actor assertion as a breach.

3.1 INC-2026-W32-01: RansomHouse Claims Fidelity Services Group [CLAIMED]

Sector	Security and Facilities Services (fidelity-services.com)
Date	Leak-site claim discovered 15 July 2026 19:28 UTC; estimated attack date 12 July 2026; first retrievable in the SA country feed on 2 August 2026
Claimed	Data theft with publication threatened; leak screenshot indexed by ransomware.live
Victim profile	Southern Africa's largest integrated security solutions provider; over 60 years of operation; guarding, cash management and fire protection across roughly 142 points of presence
Complication	ransomware.live flags the record as a possible duplicate of an existing fidelity-services.com entry claimed by the Cmdorganization group on 28 June 2026
Adjacent exposure	HudsonRock infostealer telemetry on the same record reports 1 compromised employee, 1 compromised user and 15 third-party employee credentials associated with the domain
Confidence	CLAIMED (threat-actor assertion indexed by a single aggregator; no victim statement located; duplicate flag unresolved)

RansomHouse claimed Fidelity Services Group on 15 July 2026, with the aggregator estimating the underlying attack at 12 July.² The claim did not appear in the South African country feed this report checks weekly until the 2 August retrieval, which is why it is reported here and not in W30 or W31.¹ Two cautions belong on the record. First, ransomware.live itself marks the entry as a possible duplicate of a Cmdorganization listing against the same domain dated 28 June. That flag does not exclude a genuine second compromise: an organisation can be hit twice, or claimed twice off one intrusion. Second, no public statement from Fidelity has been located, and the company has not denied the claim either. It leads the section on the strength of the victim profile. A guarding and cash-in-transit operator holds the data that describes how its clients' premises are protected: site rosters, patrol schedules, access-control records, identity documents and frequently biometric enrolments. If the claim is sound, the downstream risk reaches the physical security posture of every protected site described in the stolen material, well beyond POPIA exposure. Organisations contracting Fidelity should ask in writing what data is held on their staff and premises, and should review access-control and alarm-response arrangements on the assumption that scheduling data may be known to a third party. **Detection relevance:** run TH-2026-W32-07, since an exfiltration-led actor produces no encryption event.

3.2 INC-2026-W32-02: IncRansom Claims Reatile Group [CLAIMED]

Sector	Energy and Resources / Investment Holdings (reatile.co.za)
Date	Leak-site claim 18 July 2026; reported by DeXpose 19 July 2026
Claimed	Data theft with publication threatened; actor statement quoted as 'The full leak will be published soon, unless a company representative contacts us via the channels provided.'
Victim profile	Black-owned investment holding company established in 2003, active in South Africa's energy sector
Corroboration	Threat-intelligence aggregators (DeXpose, ransomware.live); no victim statement located
Confidence	CLAIMED (threat-actor assertion only)

IncRansom announced a claim against Reatile Group on 18 July 2026, with DeXpose publishing the incident record the following day and quoting the actor's publication threat verbatim.³ The listing also appears in the ransomware.live South African feed.¹ No Reatile statement has been located and the claim is unverified. The sector placement is what makes it worth tracking: an energy-sector investment holding company sits upstream of operating assets and typically holds transaction documentation, financing structures and counterparty detail across a whole portfolio, so the value of any exfiltrated dataset sits in commercially sensitive material more than in bulk consumer records. IncRansom operates a conventional double-extortion model with a contact-us-or-we-publish posture. Counterparties and portfolio companies should assume that correspondence and contractual material naming them may be in the actor's hands and should be alert to business email compromise attempts referencing genuine transaction detail. **Detection relevance:** TH-2026-W32-07 for bulk outbound transfer to cloud storage.

3.3 INC-2026-W32-03: Payload Claims CKR Consulting Engineers [CLAIMED]

Sector	Engineering / Professional Services (ckr.co.za)
Date	Leak-site claim discovered 19 July 2026
Claimed	Data theft with publication threatened; leak screenshot indexed
Victim profile	Johannesburg-headquartered multi-disciplinary engineering consultancy covering electrical, electronic, mechanical, renewable energy and civil engineering
Corroboration	ransomware.live South African country feed; no victim statement located
Confidence	CLAIMED (threat-actor assertion only)

The Payload group claimed CKR Consulting Engineers on 19 July 2026.¹ No victim statement has been located. Engineering consultancies are a recurring target because of what they hold on behalf of others: as-built drawings, single-line diagrams, control-system specifications and site layouts for client facilities, frequently including public infrastructure and industrial plant. That material describes the physical and control architecture of third-party sites, which is worth more than extortion leverage over the consultancy itself. Clients of CKR with renewable-energy or industrial control work in progress should establish what project documentation the firm holds and whether it would warrant a site-level risk review if published. **Detection relevance:** TH-2026-W32-07, plus file-server access auditing on project archives.

3.4 INC-2026-W32-04: M3rx Claims SuppCenter Global Services [CLAIMED; attribution caution]

Sector	Professional Services / Business Process Outsourcing (suppcentersa.com)
Date	Leak-site claim discovered 17 July 2026
Claimed	Data theft; the listing carries a partially redacted record-count teaser
Attribution caution	This report rejected an M3rx South African country tag in W30 as mis-tagged; the present listing carries a .com domain with an 'sa' string and a ZA country tag that this report cannot independently confirm as a South African legal entity
Corroboration	ransomware.live South African country feed only
Confidence	CLAIMED (threat-actor assertion only; South African nexus itself unconfirmed)

M3rx claimed SuppCenter Global Services on 17 July 2026 and the entry carries a South African country tag.¹ It is recorded so that the delta in the country tally is fully accounted for, with an explicit caution: this report rejected an M3rx South African tag in W30 as an aggregator mis-attribution, and the same doubt applies here. The domain is a .com, not a .co.za, and no South African registration, address or media footprint for the entity has been confirmed from open sources. Treat the South African nexus of this item as unconfirmed and exclude it from any count of confirmed domestic victims.

3.5 INC-2026-W32-05: SARS AI-Generated Refund Phishing Wave [CONFIRMED]

Sector	Cross-sector consumer and employee fraud; impersonation of the South African Revenue Service
Date	SARS scam alert published 28 July 2026; national media coverage 30 July 2026
Confirmed	Official SARS alert describing an active SMS and email wave claiming a refund is owed, one specimen quoting R48 900, directing recipients to a fraudulent website
Novel element	SARS states that scammers are now using AI to generate professional-looking email templates that are harder to identify as fraudulent
Timing	Peak 2026 individual filing season, when taxpayers are actively expecting SARS correspondence and refund notifications
Reporting channel	phishing@sars.gov.za; Fraud and Anti-Corruption Hotline 0800 00 2870
Confidence	CONFIRMED (primary source: SARS's own published alert, corroborated by national broadcast media)

On 28 July 2026 SARS published a scam alert headed 'Tax Return Notification', describing a wave of SMS and email messages telling recipients they are owed a refund and directing them to a fraudulent site to claim it.⁴ The alert's substantive contribution is not the existence of refund phishing, which is perennial, but the revenue service's explicit attribution of a quality step-change to generative AI: SARS records that 'the scammers are now using AI to generate professional-looking email templates that are harder to identify as fraudulent'.⁴ Eyewitness News reported the warning on 30 July, quoting SARS's instruction to delete and block.⁵ The operational consequence for South African security teams is that it invalidates the

dominant piece of consumer security advice in the country. Awareness training here has leaned heavily on language cues: spelling errors, awkward phrasing, generic salutations. Those are precisely the cues a language model removes. The replacement guidance has to be about the channel: never authenticate through a link in an unsolicited message, always type the eFiling address by hand, and treat any quoted refund amount as unverified until it is seen inside the authenticated portal. **Detection relevance:** TH-2026-W32-04 carries the mail, DNS and proxy indicators for this campaign. The employee-facing risk extends beyond personal loss, because a staff member who enters eFiling credentials on a cloned site has handed over a credential set that is frequently reused against corporate accounts.

Carryover Status (checked 2 August 2026)

Rectron / DragonForce: no development in the window. The most recent public position remains the company's 22 July recovery statement, promising containment, forensic investigation and rolling updates as verified information becomes available, with no completion announcement, no scope disclosure, no DragonForce leak-site listing naming Rectron, and no Information Regulator or Mustek statement since.¹³ **Isegen / DragonForce:** unchanged; the actor's 6 August 2026 publication deadline for the claimed 234.63 GB has not yet arrived and the victim's denial stands. **BE Travel / Arcus Media:** no delayed publication observed and no Housing Development Agency statement; publication remains UNCONFIRMED twelve days past the lapsed deadline. **Qilin / Recsa:** no corroboration and no denial; the claim is unmoved and no dataset has been published. **Profmed / PPS Healthcare Administrators:** no development and no Information Regulator statement; the administered-scheme scope remains neither confirmed nor excluded at nine weeks, and remains the most durable unresolved South African exposure in the series. **Gauteng e-Government jobs portal:** no development beyond the 14 July disclosure. **Standard Bank / Liberty (Prinz Eugen / ROOTBOY):** listing unchanged and unretracted.¹ **AVBOB Mutual Assurance:** approximately nine weeks post-incident with no leak-site claim; UNDETERMINED. **#OpSouthAfrica:** no activity since May 2026; Department of Correctional Services data remains in actor hands, so the matter is dormant. **SAPS Western Cape POPIA breach, Tembisa Hospital prosecution and ICASA / Session Telecoms:** no published outcomes.

13. IT-Online, Rectron goes into recovery mode after cyber attack (22 July 2026; W31 carryover). <https://it-online.co.za/2026/07/22/rectron-goes-into-recovery-mode-after-cyber-attack/>

4. THREAT ACTORS

4.1 RansomHouse [CLAIMED activity against SA]

RansomHouse is the most consequential actor against South Africa on this week's visible record, by virtue of its 15 July claim against Fidelity Services Group.² The operation runs a data-theft and extortion model that historically emphasises exfiltration and publication pressure over encryption, which is significant for detection: a victim may experience no service disruption at all and learn of the intrusion only when it is named on a leak site. That profile is consistent with the absence of any public statement from Fidelity. For South African defenders the practical implication is that RansomHouse activity will not announce itself through ransomware symptoms. The detectable signal is bulk outbound transfer and anomalous access to file shares.

4.2 IncRansom [CLAIMED activity against SA]

IncRansom claimed Reatile Group on 18 July with a standard contact-us-or-we-publish ultimatum.³ The group operates conventional double extortion and has been observed against professional-services and holding-company targets where document archives are the prize. Its appearance in the South African feed alongside Payload and M3rx in a single three-day span reinforces a pattern this report has noted repeatedly: South Africa is not dominated by one or two ransomware brands but is worked by a long tail of mid-tier operations, which makes actor-specific defence less useful here than generic exfiltration detection.

4.3 Payload [CLAIMED activity against SA]

Payload claimed CKR Consulting Engineers on 19 July.¹ The group is a comparatively low-profile operation and this is its first appearance in this series against a South African target. Engineering and architectural consultancies are a recurring victim class for smaller operations because they combine valuable third-party documentation with security programmes sized for a professional-services firm, well below what the critical infrastructure in their drawings would warrant.

4.4 DragonForce [CONFIRMED activity against SA; carryover]

DragonForce remains the most significant confirmed actor against South Africa in the current series, named by Rectron as the suspected group behind its confirmed breach and claiming Isegen South Africa.¹³ Neither position moved in this window. The 6 August publication deadline for the claimed Isegen dataset falls inside the coming week and is the single most likely source of a resolution to the victim-denial-versus-actor-claim conflict. Affiliate tradecraft of note for hunting purposes remains the abuse of signed but vulnerable Microsoft-ecosystem drivers to disable endpoint protection ahead of mass file access.

4.5 Arista VeloCloud Orchestrator Zero-Day Operator [CONFIRMED exploitation; UNATTRIBUTED]

An unattributed actor exploited CVE-2026-16812 (CVSS 10.0), an OS command injection in Arista VeloCloud Orchestrator On-Prem, as a zero-day before the vendor's disclosure; CISA added it to the KEV catalogue on 27 July with a 30 July remediation date.⁶⁷ Arista published three IP addresses linked to the attacks, namely 8.19.75.217, 206.72.242.124 and 206.72.242.162, and advised customers to block them and review logs.⁶ No actor name, victim set or geography has been published, and no South African victim is known. The exposure is nonetheless directly relevant to South African enterprises and managed service providers running on-premises SD-WAN orchestration, because compromise of an orchestrator is compromise of the control plane for every branch it manages. Affected trains are VCO 5.2.x below 5.2.3.14, 6.1.x below 6.1.3.4, 6.4.x below 6.4.2.4 and 7.0.x below 7.0.0.1; hosted and dedicated instances were patched by the vendor.⁷

4.6 Check Point SmartConsole Exploiters [CONFIRMED exploitation; broadened by public PoC]

The unattributed operator exploiting Check Point SmartConsole CVE-2026-16232 to obtain a full administrative token, first reported in W31, saw its effective attacker pool widen this week: Rapid7 published a working proof-of-concept on 29 July.¹¹ The six attacker IPs published by Check Point remain valid indicators and have not expanded. The material change for South African defenders is that exploitation is no longer confined to whoever developed the original capability. From 29 July onward any competent operator can reproduce it, and the KEV deadline of 25 July is long past. Separately, and not to

be conflated with this CVE, vendor research published on 27 July documents a confirmed Qilin affiliate exploiting a different Check Point flaw, the IKEv1 VPN authentication bypass CVE-2026-50751, in post-compromise activity.¹²

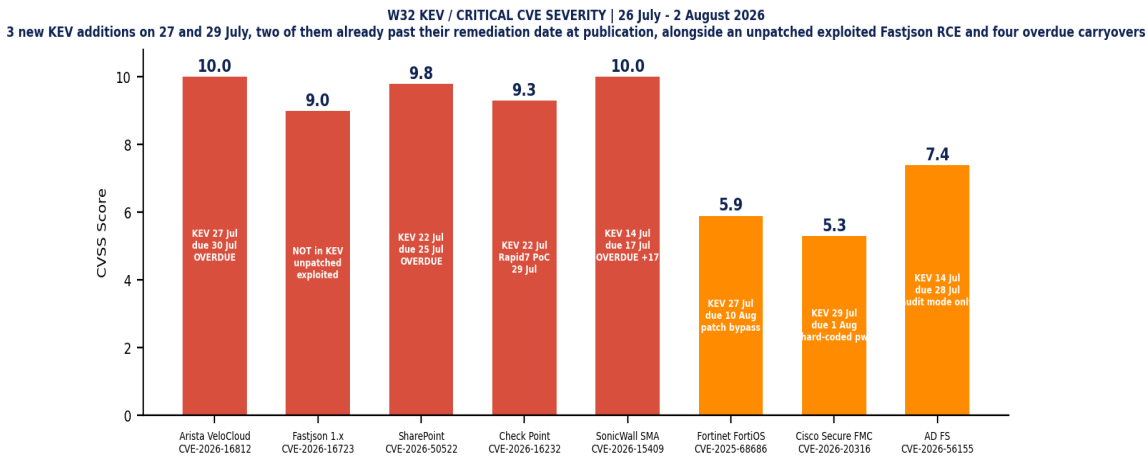
4.7 Fastjson Exploiters [CONFIRMED exploitation; no patch available]

Threat actors are exploiting CVE-2026-16723 (CVSS 9.0), an unauthenticated remote code execution flaw in Alibaba's Fastjson 1.x JSON library, for which no fix is available.¹⁰ Alibaba's own advisory notes the flaw is exploitable under Fastjson's stock default configuration, with no AutoType enablement and no classpath gadget required, affecting versions 1.2.68 to 1.2.83 in Spring Boot fat-JAR deployments with SafeMode at default.¹⁰ Exploitation has been reported by ThreatBook and Imperva against financial services, healthcare and retail targets, although neither firm has published victim names or proof of successful code execution as distinct from attempted exploitation, and the flaw was absent from the KEV catalogue as of the reporting date.¹⁰ Fastjson is widely embedded in Java estates across South African financial services and telecommunications, frequently as a transitive dependency that application owners are unaware of. Interim mitigation is to set the JVM property `fastjson.parser.safeMode` to true, or to move to the 1.2.83_noneautotype artefact.

5. CRITICAL VULNERABILITIES & CISA KEV

Three vulnerabilities entered the CISA KEV catalogue between 26 July and 2 August 2026, against six the previous week, the lowest weekly count since W28.⁶⁸⁹ The count says less than the timing. Two of the three carried remediation dates that had already passed by the time this report reached a reader: Arista VeloCloud Orchestrator On-Prem CVE-2026-16812 (CVSS 10.0, OS command injection) was added on 27 July with a 30 July date, and Cisco Secure Firewall Management Center CVE-2026-20316 (hard-coded password, CVSS 5.3) was added on 29 July with a 1 August date.⁹ The third, Fortinet FortiOS CVE-2025-68686, is a February-patched SSL-VPN information-disclosure flaw that allows an attacker who has already achieved file-system access to bypass the patch for the symbolic-link persistence mechanism; its date is 10 August.⁷ All three are network-edge or security-management products. Two further items belong alongside them although neither is in the catalogue: the unpatched and actively exploited Fastjson RCE CVE-2026-16723,¹⁰ and the Rapid7 proof-of-concept published on 29 July for the already-KEV-listed Check Point SmartConsole flaw.¹¹ A procedural note for compliance tracking: the KEV required-action text now references Binding Operational Directive 26-04, replacing the long-standing BOD 22-01, and remediation dates are set per entry, not on a uniform interval, so a fixed three-week assumption in a patch-management SLA will produce false compliance.⁹

W32 KEV / Critical CVE Severity Overview: 3 New KEV Adds Plus Unpatched and Overdue Items



W32 CISA KEV / Critical CVE Tracking (new adds 27-29 July plus active carryovers)

CVE	Vendor / Product	CVSS	Type	KEV Due	Notes
CVE-2026-16812	Arista VeloCloud Orchestrator On-Prem	10.0	OS command injection	30 Jul	KEV 27 Jul. OVERDUE at publication. Vendor-confirmed zero-day. Attacker IPs published: 8.19.75.217, 206.72.242.124, 206.72.242.162. Fixed in 5.2.3.14 / 6.1.3.4 / 6.4.2.4 / 7.0.0.1.
CVE-2026-20316	Cisco Secure Firewall Management Center	5.3	Hard-coded password	1 Aug	KEV 29 Jul. OVERDUE at publication. Cisco PSIRT confirmed exploitation in July. Check /var/tmp/license.tmp references; rotate all credentials, keys and certificates. Hot fixes for 7.0-7.7 and 10.0.
CVE-2025-68686	Fortinet FortiOS SSL-VPN	5.9	Info disclosure (patch bypass)	10 Aug	KEV 27 Jul. Bypasses the symlink-persistence patch; requires prior file-system compromise. Patched by Fortinet in Feb 2026 (FG-IR-25-934). Low CVSS, high post-exploitation value.

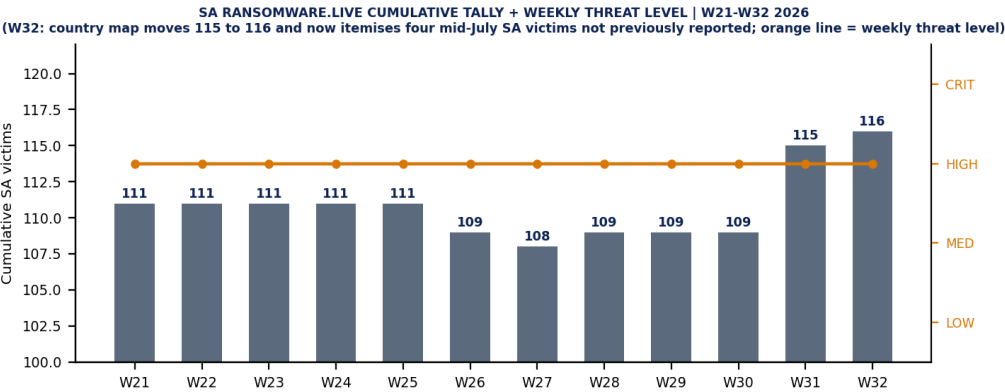
CVE-2026-16723	Alibaba Fastjson 1.x	9.0	Unauth RCE (deserialization)	n/a	NOT IN KEV. No patch available. Exploitable in stock default config, versions 1.2.68–1.2.83. Mitigate with fastjson.parser.safeMode=true. Often a transitive dependency.
CVE-2026-16232	Check Point SmartConsole	9.3	Improper auth	25 Jul	OVERDUE +9. Rapid7 PoC published 29 Jul widens the attacker pool. Six attacker IPs unchanged. Hunt for issued admin tokens as well as confirming patch level.
CVE-2026-50522	Microsoft SharePoint Server	9.8	Deserialization RCE	25 Jul	OVERDUE +9. Machine-key theft in a single request; EPSS 57.1%. Patch AND rotate ASP.NET machine keys estate-wide. No confirmed ransomware linkage.
CVE-2026-15409	SonicWall SMA 1000	10.0	SSRF (unauth)	17 Jul	OVERDUE +17. UTA0533 zero-day chained with CVE-2026-15410 (CVSS 7.2) for root. ORANGETAIL is the webshell, not the actor. Root access reaches stored and cached credentials, so rebuild the appliance; patching in place is insufficient.
CVE-2026-56155	Microsoft AD Federation Services	7.4	Priv escalation	28 Jul	Deadline PASSED in window. July update ships AUDIT MODE ONLY; enforcement deferred to 13 Oct 2026. Set RemediateDkmAcl manually; watch AD FS Admin Event IDs 1132-1136.
CVE-2026-46817	Oracle E-Business Suite	n/a	Improper privilege mgmt	18 Jul	OVERDUE +16. Not CIOp-linked: do not conflate with the 2025 CVE-2025-61882 campaign. Re-verify against the 21 Jul CPU's 410 EBS patches.
CVE-2026-60137	WordPress Core	5.9	SQL injection	4 Aug	Deadline falls the day after publication. Second half of the wp2shell chain. Confirm on self-hosted and agency-managed estates now.

Pattern note: W32's signal is that the remediation window has closed faster than the reporting cycle. Two of the three new KEV entries expired before this report could be read, which means a weekly patch cadence can no longer meet KEV dates for edge appliances. Remediation has to be driven by the vendor

advisory and the KEV feed directly. Add an exploited flaw with no patch at all (Fastjson), a public exploit released for an already-overdue management-plane bug (Check Point), and an AD FS deadline that passed while the shipped mitigation runs in audit mode only until October, and four of this week's tracked items cannot be closed by patching inside the deadline even by a well-run team. Prioritise by what an attacker gains: control-plane compromise (Arista, Cisco FMC, Check Point) above data-plane exposure, with assume-compromise handling for the SonicWall and Oracle items, seventeen and sixteen days overdue respectively.

6. RANSOMWARE LANDSCAPE

The ransomware.live South African country map reported 116 cumulative victims when retrieved on 2 August 2026, against the 115 this report recorded from the country-statistics page on 26 July.¹ The net movement is +1. The composition is what changed. The retrieved page now itemises four South African listings dated 15 to 19 July 2026 that were not retrievable from the same source a week earlier: Fidelity Services Group / RansomHouse (15 July), SuppCenter Global Services / M3rx (17 July), Reatile Group / IncRansom (18 July) and CKR Consulting Engineers / Payload (19 July).¹²³ Not one of them was visible during the W30 or W31 retrievals in which they should have appeared. Meanwhile the most recent South African entry on the map is dated 19 July, a fourteen-day gap to the 2 August retrieval. Separately, Qilin's 22 July claim against Recsa, reported in W31 from a different source, has still not propagated after eleven days. Together these two observations put a number on a caveat this report has carried since W25: the South African country feed runs roughly two to three weeks behind the leak sites it aggregates, and it back-fills. The operational posture that follows is to treat any week's South African total as a provisional floor that will be revised upward, and to read a week with no new listings as information about the feed.



Baseline (W31)	115 cumulative SA victims (country-statistics page, retrieved 26 July 2026)
Current (W32)	116 cumulative SA victims (country map, retrieved 2 August 2026)
Claims dated inside the window	0. No South African listing dated 26 July to 2 August 2026 was observed
Listings newly surfaced	4, all dated 15-19 July 2026: Fidelity Services Group / RansomHouse; SuppCenter Global Services / M3rx (ZA nexus unconfirmed); Reatile Group / IncRansom; CKR Consulting Engineers / Payload
Delta explanation	The +1 net movement understates activity. Four mid-July listings became visible while earlier entries aged out of the displayed set. The feed is back-filling
Lag measurement	Most recent SA entry on the map is dated 19 July; the Qilin / Recsa claim of 22 July reported in W31 has not propagated after 11 days. Observed feed lag is 11 to 14 days
Carryover positions	Rectron confirmed, still unlisted by DragonForce; Isegen claim live with a 6 August deadline; BE Travel publication unconfirmed 12 days past deadline; Recsa uncorroborated
Threat-level drivers	Four newly surfaced SA victims including the largest regional security provider; two KEV items overdue at publication; unpatched exploited Fastjson RCE; new public exploit for Check Point

Group notes: **RansomHouse:** first appearance against a major South African target in this series; exfiltration-led model with limited encryption, so expect no service-disruption signal (Section 4.1).² **IncRansom** and **Payload:** mid-tier operations claiming Reatile and CKR within a day of each other, consistent with the long-tail targeting pattern this report has described (Sections 4.2, 4.3). **DragonForce:** unmoved on both Rectron and Isegen; the 6 August Isegen deadline is the week's key date (Section 4.4). **Qilin:** no new South African claim; Recsa remains uncorroborated, and vendor research this week confirms Qilin affiliates exploiting Palo Alto GlobalProtect CVE-2026-0257 and Check Point CVE-2026-50751 for initial access, which is the more useful intelligence for South African defenders than the victim count.¹² **Arcus Media:** BE Travel publication still unconfirmed. **Prinz Eugen / ROOTBOY:** Standard Bank / Liberty listing unchanged.¹

7. OSINT EXPOSURE & ATTACK SURFACE

South African domains serving as phishing infrastructure

Weekly phishing-as-a-service tracking for 20 to 26 July 2026 records 7,295 tracked kit uploads globally and lists two South African domains among the indicators for the EvilTokens kit: careldutoit-el[.]co[.]za and eqfit[.]co[.]za.¹⁴ Both are ordinary South African business domains appearing in an attacker infrastructure list, which almost always means the underlying hosting or CMS was compromised and repurposed, with no complicity by the businesses themselves. This matters for two separate reasons. For the domain owners, a compromised site hosting a Microsoft 365 credential-harvesting page is a reportable security compromise with reputational and POPIA consequences. For everyone else, it is evidence that .co.za domains are being used to lend local legitimacy to phishing aimed at South African recipients, so allow-listing by country-code top-level domain is not a control. Exposure action: block both domains, and run the W30 owned-domain and CMS inventory again with specific attention to any hosting

you no longer actively maintain.

Device-code and adversary-in-the-middle phishing against Microsoft 365

The same tracking shows OAuth device-code phishing at 2,446 weekly uploads and rising by 194 week-on-week, now the primary adversary-in-the-middle technique ahead of classic credential-harvesting pages.¹⁴ The Greatness kit, which pre-fills the victim's email address and injects the target company's real logo, is documented as concentrating on manufacturing, healthcare and technology firms specifically in the United States, United Kingdom, Australia, South Africa and Canada, with South Africa named explicitly among five target countries.¹⁴ Device-code abuse defeats one-time-password and push-based multi-factor authentication entirely, because the victim approves a genuine Microsoft prompt. Exposure action: restrict or disable the OAuth device-code flow in Entra ID Conditional Access unless an IoT or CLI workflow requires it; deploy phishing-resistant FIDO2 or passkey authentication for privileged accounts; and alert on device-code sign-ins from accounts that have never used the flow. Read this alongside the SARS campaign in Section 3.5, because the same AI-assisted lure quality is being applied to both consumer tax fraud and corporate credential theft.

Edge VPN and firewall appliances as the ransomware front door

Vendor research published on 27 July 2026 consolidates four converging campaigns against internet-facing remote-access infrastructure and concludes that these appliances have become the ransomware ecosystem's preferred initial-access vector.¹² The components are the Fortibleed mass credential exposure affecting an estimated 30,791 to 75,000 FortiGate devices across 194 countries and more than 21,000 domains, roughly half of all internet-facing FortiGate appliances visible on Shodan, plus Qilin-affiliate exploitation of Palo Alto GlobalProtect CVE-2026-0257 and Check Point CVE-2026-50751, and a CitrixBleed-family NetScaler flaw CVE-2026-8451 that saw exploitation attempts within 24 hours of disclosure.¹² South African relevance is direct: FortiGate is heavily represented in the local mid-market and managed-service estate, and any organisation appearing in the exposed dataset should treat its perimeter credentials as compromised. Exposure action: rotate every FortiGate administrator and SSL VPN password, upgrade to a supported FortiOS release and force each administrator to log in once afterwards to trigger PBKDF2 re-hashing, remove management interfaces from internet exposure, and hunt for unexpected admin logins.

Infostealer credentials preceding leak-site listings

The Fidelity Services Group victim record carries associated infostealer telemetry reporting one compromised employee, one compromised user and fifteen third-party employee credentials tied to the domain.² Infostealer log purchases routinely precede ransomware intrusion by weeks, which makes credential-exposure monitoring one of the few predictive controls available. Exposure action: query an infostealer credential feed for your own and your key suppliers' domains monthly, and treat any hit as a mandatory password reset plus session revocation, never an advisory.

14. Cyber Security News, Top 10 phishing kits used by hackers, week of 20-26 July 2026; SA-hosted EvilTokens infrastructure and Greatness targeting of South Africa (28 July 2026). <https://cybersecuritynews.com/top-10-phishing-kits-used-by-hackers/>

8. REGULATORY & POLICY

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

The Information Regulator's media-statements index, checked on 2 August 2026, carries no publication later than 2 June 2026, when the Regulator announced enforcement notices for POPIA and PAIA contraventions by public and private bodies.¹⁵ That is nine weeks of public silence, across a period containing a confirmed provincial-government identity-document breach, a confirmed national technology-distributor breach with acknowledged regulator notification, and now four unacknowledged ransomware claims against South African companies. The point this report has made in each of the past three editions holds: absence of publication is not evidence of inactivity, since investigations are not published in progress, but without recent precedent a responsible party deciding whether a compromise meets the section 22 threshold has nothing contemporary to calibrate against, and the conservative reading, which is to notify, remains defensible. A sharper issue arises this week: four South African companies are publicly named on ransomware leak sites and none has made any statement. Section 22 obliges notification to the Regulator and to affected data subjects as soon as reasonably possible after there are reasonable grounds to believe personal information has been accessed by an unauthorised person. A public listing naming the organisation is, at minimum, a trigger to investigate whether those grounds exist.

FIC Directive 11 Risk and Compliance Return: second deadline passed 31 July 2026 [CONFIRMED]

The Financial Intelligence Centre's second Risk and Compliance Return deadline under Directive 11 closed at 17:00 on Friday 31 July 2026 for legal practitioners (Item 1), estate agents (Item 3), non-casino gambling institutions (Item 9) and high-value goods dealers including dealers in precious metals, precious stones and Krugerrands (Item 20), covering reporting periods running from 2023 to March 2026.¹⁶ The FIC's published position is that failure to submit may lead to administrative action, and a separate return is required per accountable institution against its own organisation identity number, including for institutions with branch networks and those operating across more than one Schedule 1 item.¹⁶ No enforcement outcome has been published as at 2 August. Affected institutions that did not submit should not wait to be contacted: prompt voluntary regularisation is the posture that mitigates sanction, and boards should obtain written confirmation of submission status. This closes out the forward-looking item carried in W31.

SARS as a public-body fraud warning with private-sector consequences [CONFIRMED]

The SARS scam alert of 28 July is a consumer-protection communication carrying no regulatory force, but it carries a governance implication for South African employers.⁴ Tax-season impersonation targets employees on personal devices and personal accounts, and the credential sets harvested are frequently reused against corporate systems. An employer that does not brief staff on a nationally publicised, government-confirmed fraud wave during filing season is accepting a foreseeable and cheaply mitigated risk. Where an organisation holds employee tax information, and payroll bureaux, employers of record and outsourced HR providers are the obvious cases, the same campaign also constitutes a plausible pretext for social engineering against the finance function itself, and warrants a specific control on out-of-band

verification for any tax-related payment or banking-detail instruction.

15. Information Regulator (South Africa), Media statements index; latest 2026 statement dated 2 June 2026 (checked 2 August 2026). <https://infoeregulator.org.za/media-statements/>

16. Financial Intelligence Centre, 2026 Risk and Compliance Return, Directive 11 submission deadlines (checked 2 August 2026). <https://www.fic.gov.za/risk-and-compliance-return-submissions/>

9. WEEKLY THREAT HUNT & IOCs

The W32 hunt set is weighted towards remediation that has already run out of time. Three P1 missions cover the two KEV items that lapsed before publication, Arista VeloCloud and Cisco Secure FMC, and the SonicWall SMA 1000 campaign now seventeen days past its date. Two P2 missions cover the SARS AI-generated phishing wave, the highest-volume domestic threat of the week, and the OAuth device-code and adversary-in-the-middle activity that names South Africa as a target country. Two P3 missions cover the unpatched Fastjson RCE and exfiltration-led ransomware, which produces no encryption signal at all. Atomic indicators are available for TH-01 (three attacker IPs), TH-03 (file paths and a request signature published by Volexity¹⁷) and TH-05 (nine kit domains); the remainder are behavioural. A machine-readable indicator export accompanies this report (iocs_w32.csv).

17. The Hacker News, SonicWall SMA zero-days exploited before disclosure to gain root access; Volexity attribution of UTA0533 (19 July 2026). <https://thehackernews.com/2026/07/sonicwall-sma-zero-days-exploited.html>

TH-2026-W32-01: Arista VeloCloud Orchestrator
CVE-2026-16812 Zero-Day Hunt

P1 CRITICAL: CVSS 10.0;
vendor-confirmed zero-day; KEV due 30
Jul (LAPSED); SD-WAN control plane

Hypothesis: An unauthenticated attacker exploits an OS command injection flaw in on-premises VeloCloud Orchestrator to execute commands with privileged access on the orchestrator host. Because the orchestrator is the control plane for every branch edge it manages, a single compromise yields configuration control, credential material and a trusted pivot into every managed site simultaneously.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1078 (Valid Accounts), T1552 (Unsecured Credentials), T1199 (Trusted Relationship).

IOCs: Attacker IPs published by Arista (block and retro-hunt): 8.19.75.217, 206.72.242.124, 206.72.242.162. Also: unexpected shell processes spawned by orchestrator services; new or modified administrative accounts on the VCO; configuration pushes to edge devices with no change ticket; outbound connections from the orchestrator to unfamiliar destinations.

Data Sources: VCO application and system logs, orchestrator host EDR telemetry, perimeter netflow and firewall logs, SD-WAN configuration change history, management-segment authentication logs.

Detection Guidance: Upgrade to 5.2.3.14, 6.1.3.4, 6.4.2.4 or 7.0.0.1 as applicable, since the 30 July KEV date has passed. Block the three published IPs and search historical netflow back to at least early July for any connection from them. Because this was exploited as a zero-day before disclosure, patch level does not establish innocence: review orchestrator account inventory and every edge configuration change in the period, and rotate orchestrator credentials and any device certificates it can issue.

TH-2026-W32-02: Cisco Secure FMC CVE-2026-20316 Hard-Coded Credential Hunt

P1 CRITICAL: exploitation confirmed by
Cisco PSIRT; KEV due 1 Aug (LAPSED);
security management plane

Hypothesis: An attacker authenticates to Cisco Secure Firewall Management Center using a static, hard-coded credential present in the shipped software, obtaining access to the management plane that controls firewall policy for the estate. As with any management-plane compromise, the blast radius is the whole protected network rather than a single host, and the access is indistinguishable from legitimate administration in most logging.

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

IOCs: Vendor-published forensic artefact: references to /var/tmp/license.tmp in FMC logs, retrievable in expert mode with 'cat /var/log/messages | grep license'. Also: FMC logins outside known administrator source ranges; firewall policy or access-control-list changes with no corresponding change record; new FMC user accounts; unexpected deployment pushes to managed devices.

Data Sources: FMC /var/log/messages and audit logs, FMC policy deployment history, management-segment netflow, SIEM correlation on FMC authentication events, change-management records.

Detection Guidance: Apply the hot fix for your FMC train (7.0, 7.2, 7.4, 7.6, 7.7 or 10.0), since the 1 August KEV date has passed. Run the license-log check and treat any /var/tmp/license.tmp reference as possible compromise. Cisco advises rotating all credentials, keys and certificates on the appliance; do that, and do not assume the patch is sufficient. Re-baseline deployed firewall policy against your intended configuration.

TH-2026-W32-03: SonicWall SMA 1000 UTA0533 Assume-Compromise Hunt

P1 CRITICAL: CVSS 10.0; KEV OVERDUE
+17; root access achieved; rebuild
required

Hypothesis: Volexity attributes exploitation of CVE-2026-15409 (CVSS 10.0, a pre-authentication /wsproxy bypass) chained with CVE-2026-15410 (CVSS 7.2, path traversal in the ctrl-service remove_hotfix workflow) to UTA0533, active from 22 June 2026 and before public disclosure. The actor obtained root, wrote a setuid binary and a Python dropper containing two JAR payloads, and on a second appliance ran tcpdump against unencrypted LDAP traffic to harvest usernames and passwords. With root, stored and cached appliance credentials are reachable, so patching in place does not evict the actor.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1505.003 (Web Shell), T1040 (Network Sniffing), T1552 (Unsecured Credentials), T1546 (Event Triggered Execution), T1133 (External Remote Services).

IOCs: File paths published by Volexity: /usr/bin/xzfind (ROOTRUN setuid binary), /usr/lib/python3.11/site-packages/deploy_new.py (KNUCKLEBALL dropper), /tmp/hypdate.b64 (CVE-2026-15410 exploit), /var/tmp/lib.sh (launches tcpdump against LDAP). Config artefacts: added routes in /var/lib/unit/conf.json and a modified /etc/init.d/workplace startup script. URI paths serving the JAR payloads: /workplace/error.jsp and /workplace/dialogs/errorDialog.jsp. Request signature: unauthenticated /wsproxy request with User-Agent containing 'SMA Connect Agent' and a bmID parameter starting -3389.

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

Detection Guidance: This is seventeen days past its KEV date and should be handled as a compromise. Re-image the appliance from known-good firmware and rotate all credentials the appliance stored or processed, including directory accounts that authenticate through it. Check /var/lib/unit/conf.json for added routes and the workplace startup script for modification, then review appliance and LDAP logs from 22 June onward. Volexity assessed that the actor was less successful at lateral movement, so absence of internal spread does not rule out appliance compromise.

TH-2026-W32-04: SARS AI-Generated Refund Phishing Hunt**P2 HIGH:** government-confirmed active campaign; national scale; AI-generated lures defeat language cues

Hypothesis: Attackers distribute AI-generated SMS and email messages impersonating the South African Revenue Service, claiming a refund is owed and directing recipients to credential-harvesting sites. Because the lures are model-generated they carry correct grammar, authentic branding and genuine SARS employee names, defeating the language-error heuristics on which most South African awareness training depends. Harvested eFiling credentials are frequently reused against corporate accounts.

MITRE ATT&CK: T1566.002 (Phishing: Spearphishing Link), T1566.003 (Spearphishing via Service), T1656 (Impersonation), T1589 (Gather Victim Identity Information), T1078 (Valid Accounts).

IOCs: Inbound mail spoofing the sars.gov.za display name from non-SARS infrastructure; SPF, DKIM or DMARC failures on messages claiming SARS origin; newly registered domains containing 'sars', 'efiling' or 'sarsrefund'; message bodies quoting a specific refund amount (R48 900 in the SARS specimen); user reports of refund SMS messages; outbound connections from corporate hosts to newly registered lookalike domains.

Data Sources: Email gateway and quarantine logs, DMARC aggregate reports, web proxy logs for newly registered domain categories, DNS resolution logs, user phishing-report mailbox, identity-provider sign-in logs for impossible-travel and unfamiliar-device events following a suspected credential entry.

Detection Guidance: Issue a targeted staff advisory in the week of 3 August and change the guidance: language quality is no longer a signal, so the rule is to authenticate only at a hand-typed official address and never through an unsolicited link. Block newly registered SARS-lookalike domains at the proxy and add a display-name spoofing rule for sars.gov.za. Forward specimens to phishing@sars.gov.za. Where an employee reports entering credentials, force a corporate password reset and session revocation on the assumption of reuse.

TH-2026-W32-05: OAuth Device-Code and AiTM Phishing Hunt (SA named target)**P2 HIGH:** device-code abuse now the primary AiTM technique; SA named among five target countries

Hypothesis: An attacker sends a lure disguised as a document share, Teams invite or SharePoint access request instructing the victim to enter a device code at a genuine Microsoft URL, thereby authorising the attacker's session without ever touching a password or triggering a suspicious login page. Alternatively an AiTM reverse-proxy kit relays a real authentication and steals the post-MFA session cookie. Both defeat OTP and push-based MFA entirely.

MITRE ATT&CK: T1566 (Phishing), T1557 (Adversary-in-the-Middle), T1550.001 (Use of Application Access Token), T1539 (Steal Web Session Cookie), T1567 (Exfiltration Over Web Service).

IOCs: South African domains observed in EvilTokens infrastructure: careldutoit-el[.]co[.]za, eqfit[.]co[.]za. Other kit infrastructure: authdocspro[.]com, docusend[.]net, ssolutionmail[.]com, evobothub[.]org, m365-verification[.]ru, evilproxy[.]pro, msdnmail[.]net. Behavioural: device-code sign-ins from accounts that have never used the flow; inconsistent User-Agent strings across authentication steps within one session; new inbox rules that auto-delete or forward externally; unexpected OAuth application consent grants.

Data Sources: Entra ID sign-in logs filtered on device-code authentication, OAuth consent-grant audit logs, Microsoft Graph API activity logs for bulk mailbox reads, mailbox rule creation events, email gateway telemetry, web proxy logs.

Detection Guidance: Restrict or disable the OAuth device-code flow in Conditional Access unless an IoT or CLI workflow genuinely requires it, because this single change removes the dominant technique. Deploy FIDO2 or passkey authentication for privileged accounts. Alert on first-ever device-code use per account and on impossible device shifts within a session. Block the listed domains and audit consent grants for unrecognised applications.

TH-2026-W32-06: Unpatched Fastjson CVE-2026-16723 RCE Hunt**P3 MEDIUM:** CVSS 9.0; exploited in the wild; NO PATCH AVAILABLE; often a transitive dependency

Hypothesis: An attacker sends crafted JSON to a Java application that deserialises untrusted input using Fastjson 1.2.68 to 1.2.83, achieving unauthenticated remote code execution under the library's stock default configuration without requiring AutoType or a classpath gadget. The exposure is frequently invisible to application owners because Fastjson arrives as a transitive dependency inside a Spring Boot fat JAR.

MITRE ATT&CK: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1195.001 (Supply Chain Compromise: Software Dependencies), T1105 (Ingress Tool Transfer), T1068 (Exploitation for Privilege Escalation).

IOCs: Anomalous or malformed JSON POST bodies to API endpoints; Java application processes spawning shell children; outbound connections from application servers to unfamiliar destinations shortly after a JSON request; new files written by the JVM user; deserialization exceptions in application logs immediately preceding process anomalies.

Data Sources: Application and API gateway logs, WAF logs, JVM and application-server logs, EDR process-creation telemetry on Java hosts, software bill of materials and dependency-scanning output, egress netflow.

Detection Guidance: There is no patch, so the control is configuration and inventory. Run a dependency scan across every Java application to find Fastjson 1.x including transitive inclusions, then set the JVM property `fastjson.parser.safeMode` to true or migrate to the 1.2.83_noneautotype artefact. Place a WAF rule in front of JSON-accepting endpoints. Note that reported activity to date is observed exploitation attempts rather than proven successful execution, so calibrate urgency to your own exposure.

TH-2026-W32-07: Exfiltration-Led Ransomware Hunt (No-Encryption Signal)**P3 MEDIUM:** RansomHouse-type model; four SA victims surfaced; no service-disruption indicator

Hypothesis: An operation running a data-theft-and-extortion model without encryption is present in the environment and will exfiltrate before making any demand. Because there is no encryption event, none of the usual ransomware alarms fire and the organisation may first learn of the intrusion from a leak-site listing weeks later, which is exactly the sequence implied by four South African victims appearing publicly with no operational disruption reported by any of them.

MITRE ATT&CK: T1567.002 (Exfiltration to Cloud Storage), T1041 (Exfiltration Over C2 Channel), T1074 (Data Staged), T1005 (Data from Local System), T1039 (Data from Network Shared Drive), T1562.001 (Impair Defenses).

IOCs: Large staged archives in temporary or user directories; sustained outbound transfers to file-sharing or cloud-storage services outside business hours; mass file reads across network shares by a single account in a short window; use of `rclone`, `MEGAcmd`, `WinSCP` or similar transfer utilities in environments where they are not standard; service-account authentication to file servers it does not normally touch.

Data Sources: DLP and egress netflow, file-server access auditing, EDR process-creation and command-line telemetry, cloud access security broker logs, proxy logs for cloud-storage destinations, identity-provider logs for service accounts.

Detection Guidance: Baseline normal outbound volume per host and alert on multi-gigabyte transfers to consumer cloud storage. Enable file-server access auditing if it is off, which is the most common gap. Given four South African victims surfaced this week across security services, energy, engineering and outsourcing, prioritise this hunt in document-heavy environments, and validate that offline immutable backups exist even though the threat model here is publication of stolen data.

10. STRATEGIC RECOMMENDATIONS

Technical (SOC / IR)

- 1. Close the two lapsed KEV items on Monday 3 August and treat Arista VeloCloud as a suspected compromise.** CVE-2026-16812 (CVSS 10.0) was exploited as a zero-day before disclosure, so a current patch level does not establish that you were not hit. Upgrade, block 8.19.75.217, 206.72.242.124 and 206.72.242.162, retro-hunt netflow back to early July, and audit orchestrator accounts and edge configuration changes. For Cisco Secure FMC CVE-2026-20316, apply the hot fix, run the license-log check for /var/tmp/license.tmp, and rotate appliance credentials, keys and certificates.
- 2. Change the phishing advice you give staff in the week of 3 August.** The SARS alert confirms AI-generated lures with correct grammar and genuine branding. Retire spot-the-typo guidance and replace it with channel discipline: authenticate only at hand-typed official addresses, never through links. Pair it with device-code restriction in Entra ID Conditional Access, which removes the single most-used corporate credential-theft technique of the week, and block careldutoit-el[.]co[.]za and eqfit[.]co[.]za.
- 3. Rebuild the SonicWall SMA 1000 estate; patching in place is insufficient.** Seventeen days overdue, with confirmed root-level compromise in the reported incident and a public Rapid7 proof-of-concept. Rebuild from known-good firmware, rotate every credential the appliance stored or processed, and hunt for the ORANGETAIL and Suo5 JAR routes in /var/lib/unit/conf.json from 22 June onward.
- 4. Inventory Fastjson 1.x across your Java estate.** An exploited RCE with no available patch is a configuration and inventory problem. Run dependency scanning for transitive Fastjson inclusions, set fastjson.parser.safeMode to true, and place WAF coverage in front of JSON-accepting endpoints.
- 5. Build the exfiltration-without-encryption detection you are probably missing.** Four South African victims surfaced with no reported service disruption. Baseline outbound volume per host, alert on bulk transfers to consumer cloud storage, and enable file-server access auditing if it is not already on.

Management (CISO / Board)

- 1. Your leak-site monitoring is roughly two to three weeks out of date, and you should plan for that.** Four South African victims dated mid-July became visible only this week, and a 22 July claim reported a week ago still has not propagated. Any dashboard fed by these sources is showing you a floor. The governance consequence is that 'no news this week' does not constitute assurance, and supplier risk decisions should not rest on the absence of a listing.
- 2. A guarding and cash-in-transit provider breach carries physical security consequences as well as data ones.** The RansomHouse claim against Fidelity Services Group, unconfirmed but credible enough to act on, involves an organisation holding site rosters, access-control records and identity documents for the premises it protects. If Fidelity or a comparable provider serves your sites, ask in writing what they hold and review access-control and alarm-response arrangements on the assumption that scheduling data may be known externally. Cyber risk converts directly into physical risk here.

3. Weekly patch cadence no longer satisfies KEV deadlines for edge devices. Two of this week's three additions expired before this report reached you. If your organisation patches perimeter appliances on a weekly or fortnightly cycle, you are structurally non-compliant for this device class regardless of team quality. The fix is an exception path that lets edge and security-management appliances be patched on vendor-advisory timing instead of change-window timing. That is a governance decision to make at board level.

4. Register nine weeks of regulatory silence alongside four unacknowledged victims. The Information Regulator has published nothing since 2 June while four South African companies have been named on leak sites without comment. Do not read either fact as permission. A public listing is at minimum a trigger to investigate whether section 22 grounds exist, and the conservative notification posture remains the defensible one.

5. Confirm the FIC Risk and Compliance Return position in writing if you are in an affected category. The 31 July deadline for legal practitioners, estate agents, non-casino gambling institutions and high-value goods dealers has passed, with administrative sanction available for non-submission. If a return was missed, prompt voluntary regularisation is the mitigating posture. Obtain written confirmation of status, not a verbal assurance.

11. THREAT LEVEL ASSESSMENT

THREAT LEVEL: HIGH, 12th CONSECUTIVE WEEK

The South African cyber threat level remains **HIGH** for a twelfth consecutive week (26 July - 2 August 2026). No new leak-site claim was dated inside the window, but four previously invisible mid-July victims surfaced, including the largest integrated security provider in Southern Africa, and a government-confirmed national phishing campaign is running at scale during filing season. Escalation to **CRITICAL** was considered and rejected: none of the four listings is corroborated by a victim statement, no systemically important institution is confirmed compromised, and the KEV volume fell week on week. De-escalation is not supportable while two KEV items sit past their deadline, an exploited remote code execution flaw has no patch at all, a management-plane bug has a fresh public exploit, and the domestic victim picture is demonstrably lagging reality by two to three weeks.

Rationale

- **Four South African victims surfaced at once:** Fidelity Services Group (RansomHouse, 15 July), SuppCenter Global Services (M3rx, 17 July, ZA nexus unconfirmed), Reatile Group (IncRansom, 18 July) and CKR Consulting Engineers (Payload, 19 July). None was previously reported and none has been publicly acknowledged.
- **The most significant claim is against a physical-security provider:** a guarding and cash-in-transit operator holds access-control, roster and identity data for its clients' premises, converting a data breach into a physical-security exposure for third parties.

- **A government-confirmed AI-assisted fraud wave at national scale:** SARS formally recorded on 28 July that scammers are using AI to generate its phishing templates, invalidating the language-cue advice most South African awareness training depends on, at peak filing season.
- **Two KEV additions expired before publication:** Arista VeloCloud CVE-2026-16812 (CVSS 10.0, vendor-confirmed zero-day, due 30 July) and Cisco Secure FMC CVE-2026-20316 (due 1 August), both of them control-plane or management-plane products.
- **An exploited flaw with no patch:** Fastjson CVE-2026-16723 (CVSS 9.0) is exploited in the wild, unpatched, absent from KEV, and commonly present as an unnoticed transitive dependency in Java estates.
- **Overdue carryovers deepening:** SonicWall SMA 1000 is seventeen days past deadline and Oracle E-Business Suite sixteen, SharePoint and Check Point nine days, and the Check Point flaw gained a public Rapid7 exploit on 29 July.
- **Measurement lag quantified at two to three weeks:** the country feed back-filled four mid-July listings while a 22 July claim reported in W31 still has not propagated. Weekly SA counts should be read as a floor.
- **Regulatory signal still absent:** the Information Regulator has published nothing since 2 June, now nine weeks, across two confirmed breaches and four unacknowledged claims.

Next-Week Watch (W33)

- **Fidelity Services Group:** any company or client statement, any publication of the claimed dataset by RansomHouse, and whether the duplicate flag against the June Cmdorganization listing resolves into one intrusion or two.
- **Reatile Group, CKR Consulting Engineers and SuppCenter Global Services:** corroboration, denial or publication, and whether the SuppCenter entity has a genuine South African nexus.
- **Isegen / DragonForce, 6 August deadline:** whether DragonForce publishes the claimed 234.63 GB, which would finally resolve the victim-denial-versus-actor-claim conflict now running into its fourth week.
- **Rectron:** completion of the forensic investigation, scope of exfiltrated data, any DragonForce listing, and any Information Regulator or Mustek statement. Unmoved since 22 July.
- **SARS campaign:** whether the AI-generated wave broadens beyond refund lures into SARS-themed business email compromise against payroll functions as filing season peaks.
- **Arista VeloCloud CVE-2026-16812:** attribution, victim reporting, whether the three published IPs expand, and any evidence of South African managed-service exposure.
- **Fastjson CVE-2026-16723:** whether Alibaba ships a fix, whether CISA adds it to KEV, and whether confirmed compromises are published as distinct from attempted exploitation.
- **WordPress CVE-2026-60137:** the 4 August deadline falls the day after publication, so confirm self-hosted and agency-managed estates are patched before it passes.
- **ransomware.live and the Information Regulator:** whether the country feed propagates the Recsa claim and back-fills further South African listings, and whether the Regulator publishes anything after nine weeks, in particular on any of this week's four named companies.

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, assigned in order of first citation; each unique source appears exactly once and multiple footnotes may point to the same number. Every cited URL was directly retrieved and confirmed to contain the claim attributed to it, on 2 August 2026. Transparency notes: cisa.gov blocks direct automated retrieval from our environment, so CISA KEV facts are anchored to fetched secondary sources quoting the alerts (items 6, 7, 8 and 9), with per-CVE remediation dates taken from item 9 in preference to secondary roundups that applied a uniform interval. mybroadband.co.za also blocks retrieval and no claim rests on it. Item 4 is the source for the 116 cumulative figure and the four newly surfaced listings; the feed lag is analysed in Section 6. The South African nexus of the SuppCenter Global Services listing could not be independently confirmed and is flagged in Sections 3.4 and 6.

1. Ransomware.live, South Africa victim map: 116 cumulative victims (retrieved 2 August 2026). <https://www.ransomware.live/map/ZA>
2. Ransomware.live, Victim record: Fidelity Services Group / RansomHouse (discovered 15 July 2026; duplicate-entry flag; HudsonRock infostealer data). <https://ransomware.live/id/RmikZWxpHkgU2VydmljZXMG3JvdXBAdmFuc29taG91c2U>
3. DeXpose, IncRansom strikes South African energy-sector holding company Reatile Group (19 July 2026; claim posted 18 July). <https://www.dexpose.io/incransom-strikes-south-african-energy-leader-reatile-group/>
4. SARS, Scam alert: 'Tax Return Notification'; scammers now using AI to generate phishing templates (28 July 2026). <https://www.sars.gov.za/latest-news/scam-alert-tax-return-notification/>
5. Eyewitness News, SARS warns AI scams are targeting taxpayers (30 July 2026). <https://www.ewn.co.za/2026/07/30/sars-warns-ai-scams-are-targeting-taxpayers>
6. Security Affairs, U.S. CISA adds Arista VeloCloud Orchestrator and Fortinet FortiOS flaws to its Known Exploited Vulnerabilities catalog (28 July 2026). <https://securityaffairs.com/196130/security/u-s-cisa-adds-arista-velocloud-orchestrator-and-fortinet-fortios-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
7. The Hacker News, Attackers exploit Arista VeloCloud Orchestrator zero-day; FortiOS SSL-VPN patch-bypass added to KEV (28 July 2026). <https://thehackernews.com/2026/07/attackers-exploit-arista-velocloud.html>
8. Security Affairs, U.S. CISA adds a Cisco Secure Firewall Management Center flaw to its Known Exploited Vulnerabilities catalog (30 July 2026). <https://securityaffairs.com/196289/security/u-s-cisa-adds-a-cisco-secure-firewall-management-center-fmc-flaw-to-its-known-exploited-vulnerabilities-catalog.html>
9. Senserva, Exploited This Week: CISA KEV weekly summary and per-CVE due dates (updated 1 August 2026). <https://senserva.com/exploited-this-week.html>
10. SecurityWeek, Unpatched Fastjson vulnerability exploited in attacks (28 July 2026). <https://www.securityweek.com/unpatched-fastjson-vulnerability-exploited-in-attacks/>
11. The Hacker News, Rapid7 releases proof-of-concept for exploited Check Point SmartConsole flaw (29 July 2026). <https://thehackernews.com/2026/07/rapid7-releases-poc-for-exploited-check.html>
12. Cyber Security News, Ransomware gangs attack Palo Alto, Fortinet, Citrix and Check Point VPNs to target corporate networks (27 July 2026). <https://cybersecuritynews.com/ransomware-gangs-attack-vpn/>
13. IT-Online, Rectron goes into recovery mode after cyber attack (22 July 2026; W31 carryover). <https://it-online.co.za/2026/07/22/rectron-goes-into-recovery-mode-after-cyber-attack/>
14. Cyber Security News, Top 10 phishing kits used by hackers, week of 20–26 July 2026; SA-hosted EvilTokens infrastructure and Greatness targeting of South Africa (28 July 2026). <https://cybersecuritynews.com/top-10-phishing-kits-used-by-hackers/>
15. Information Regulator (South Africa), Media statements index; latest 2026 statement dated 2 June 2026 (checked 2 August 2026). <https://info regulator.org.za/media-statements/>
16. Financial Intelligence Centre, 2026 Risk and Compliance Return, Directive 11 submission deadlines (checked 2 August 2026). <https://www.fic.gov.za/risk-and-compliance-return-submissions/>
17. The Hacker News, SonicWall SMA zero-days exploited before disclosure to gain root access; Volexity attribution of UTA0533 (19 July 2026). <https://thehackernews.com/2026/07/sonicwall-sma-zero-days-exploited.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-W32 | Published Monday 3 August 2026