Southern Mutual Bank

51 824 753 556

Vulnerability Scan Report — Core Banking (Temenos T24) — Q2 2026

Report · synthetic assessor-grade test document

Generated 09 November 2026 · CyberSentien test harness · personalised to Southern Mutual Bank

Report ID	SOU-RPT-0104
Prepared by	Tom Bauer (Identity & Access Manager)
Classification	Internal Use Only
Status	Final
Reporting period	Q2 2026
Distribution	Control owner; Risk & Compliance; Internal Audit

1. Scope and method

This report records the results of vulnerability scan report for Southern Mutual Bank over the reporting period. Results were produced from the system of record and the tooling named below; exceptions are listed with an owner and a due date and are tracked to closure by the control owner, with second-line oversight.

2. Summary of results

Hosts scanned (authenticated)	412
Critical / high vulnerabilities open	3 / 11
Remediated within SLA	91%
Scan coverage of estate	98.6%

3. Results

Host	CVE	CVSS / severity	Vulnerability	Remediation status	Evidence
db-host-01	CVE-2026-3513	Critical 9.8	Missing security patch — vendor advisory	OPEN — beyond SLA	Patch record CHG-208300
web-host-02	CVE-2026-5905	High 7.5	Unsupported software version	Remediated 18 Oct 2026	Patch record CHG-208301
web-host-03	CVE-2026-9021	Critical 9.8	Default credentials	Remediated 17 Oct 2026	Patch record CHG-208302
db-host-04	CVE-2026-4848	Low 3.1	Unsupported software version	Remediated 26 Oct 2026	Patch record CHG-208303
db-host-05	CVE-2026-9728	Medium 5.3	Unsupported software version	OPEN — beyond SLA	Patch record CHG-208304
web-host-06	CVE-2026-2315	Low 3.1	Weak cipher suite	Remediated 24 Oct 2026	Patch record CHG-208305

Host	CVE	CVSS / severity	Vulnerability	Remediation status	Evidence
web-host-07	CVE-2026-7013	Critical 9.8	Outdated TLS configuration	Remediated 06 Nov 2026	Patch record CHG-208306
db-host-08	CVE-2026-3229	Low 3.1	Outdated TLS configuration	Remediated 02 Oct 2026	Patch record CHG-208307
web-host-09	CVE-2026-8742	Medium 5.3	Weak cipher suite	OPEN — beyond SLA	Patch record CHG-208308
app-host-10	CVE-2026-3140	High 8.1	Unsupported software version	Remediated 02 Oct 2026	Patch record CHG-208309
db-host-11	CVE-2026-1724	High 7.5	Missing security patch — vendor advisory	Remediated 09 Oct 2026	Patch record CHG-208310
web-host-12	CVE-2026-6970	Critical 9.8	Default credentials	Remediated 25 Oct 2026	Patch record CHG-208311
app-host-13	CVE-2026-5175	Low 3.1	Missing security patch — vendor advisory	OPEN — beyond SLA	Patch record CHG-208312
web-host-14	CVE-2026-5586	Low 3.1	Weak cipher suite	Remediated 05 Nov 2026	Patch record CHG-208313
app-host-15	CVE-2026-5675	High 7.5	Missing security patch — vendor advisory	Remediated 31 Oct 2026	Patch record CHG-208314
db-host-16	CVE-2026-8898	Critical 9.8	Outdated TLS configuration	Remediated 17 Oct 2026	Patch record CHG-208315
db-host-17	CVE-2026-9201	High 8.1	Missing security patch — vendor advisory	OPEN — beyond SLA	Patch record CHG-208316
db-host-18	CVE-2026-7123	Medium 5.3	Unsupported software version	Remediated 08 Nov 2026	Patch record CHG-208317

4. Findings and follow-up actions

Item	Action	Owner	Due
db-host-01	Remediate and evidence closure	Mei-Lin Tan	03 Jan 2027
db-host-05	Remediate and evidence closure	Priya Sharma	30 Dec 2026
web-host-09	Remediate and evidence closure	James O'Connor	25 Nov 2026
app-host-13	Remediate and evidence closure	David Okafor	25 Nov 2026
db-host-17	Remediate and evidence closure	Tom Bauer	05 Dec 2026

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

6. Review and approval

Role	Name	Date
Prepared by	Tom Bauer	03 Nov 2026
Reviewed by (2nd line)	Daniel Wright	06 Nov 2026
Approved by	Chief Information Security Officer	08 Nov 2026