ACME CORP

Security Posture — Executive Briefing

Reporting period Q3 2026 · Prepared by J. Rivera, CISO · Generated 2026-08-17 18:52

F

Critical · 33/100

Overall security posture is rated **Critical** (33/100) for this period. The score is driven down chiefly by 3 critical vulnerability(ies); high quantified loss exposure ($874K/yr); 1 expired certificate(s). The top risks and the prioritized actions to reduce them are summarized below.

ANNUAL LOSS EXPOSURE	CRITICAL / HIGH VULNS	VENDORS AT RISK	CERTS EXPIRED / <14D
$874K	**3 / 2**	**2**	**1 / 1**
High · FAIR	5 hosts	of 3 assessed	TLS & domains

LIVE THREAT INDICATORS

1 / 2

critical / high

TOP RISKS

Financial exposure

Quantified annual loss exposure is approximately $874K (High) — led by Ransomware (domain-wide). This is the expected cost of cyber loss events across modeled scenarios and frames where risk-reduction spend earns the most return.

Exploitable vulnerabilities

3 critical and 2 high-severity vulnerabilities are present across 5 host(s) (e.g. Apache Log4j RCE (Log4Shell)). These are directly exploitable for remote code execution or ransomware and should drive the immediate patch queue.

Certificate / domain hygiene

1 certificate(s) are already expired and 1 expire within 14 days. Each is a self-inflicted outage or browser trust-failure waiting to happen and is trivially preventable with owned renewal.

Third-party / supply chain

2 vendor(s) carry HIGH or CRITICAL residual risk (Acme Cloud Ltd, PayGate Inc). Third parties extend the attack surface and breach-notification and audit rights must be contractually enforced before deeper integration.

Active threat indicators

Live correlation surfaces 1 critical and 2 high threat indicator(s) across the environment (rogue devices, exposed services, malicious flows, ATT&CK activity). These warrant containment review now.

RECOMMENDED PRIORITIES

WHEN	OWNER	TIMEFRAME	ACTION
Immediate	IT Ops	0–7 days	Renew expired/expiring certificates and assign an owner + automated expiry alerting.

Immediate	Vuln Mgmt	0–14 days	Remediate critical vulnerabilities on exposed hosts; where patching lags, apply compensating controls (segmentation, WAF, disable service).
Immediate	SOC	0–3 days	Triage and contain the critical live threat indicators; confirm none represent an active intrusion.
Near-term	CISO / Finance	30–60 days	Fund the highest-ROI control against the top loss scenario (Ransomware (domain-wide)); track risk-reduction in dollars.
Near-term	Vendor Mgmt / Legal	30–90 days	Add security addenda (breach-notification SLA, right-to-audit, encryption/MFA) to high-risk vendors and schedule reassessment.
Ongoing	CISO	Quarterly	Re-run this briefing each reporting period and trend the posture score, financial exposure and open critical findings for the board.

FINANCIAL RISK (FAIR)

LOSS SCENARIO	ANNUALIZED LOSS
Ransomware (domain-wide)	$416K
Phishing to BEC wire fraud	$242K
Cloud bucket misconfig leak	$83K
Total portfolio ALE	**$874K**

VULNERABILITY HIGHLIGHTS

VULNERABILITY	SEVERITY	HOSTS
Apache Log4j RCE (Log4Shell)	CRITICAL	1
Microsoft RDP RCE (BlueKeep)	CRITICAL	1
MS17-010 EternalBlue	CRITICAL	1
SQL Server Unsupported	HIGH	1

THIRD-PARTY RISK

VENDOR	INHERENT	RESIDUAL
Acme Cloud Ltd	HIGH	CRITICAL
PayGate Inc	HIGH	HIGH
MailCo	MEDIUM	LOW

CERTIFICATE & DOMAIN EXPIRY

NAME	DAYS	STATUS
legacy-vpn.acme.corp	-3	EXPIRED
acme.com (registrar)	+8	URGENT
*.internal.acme.corp	+26	SOON

LIVE THREAT INDICATORS

INDICATOR	SEVERITY	TARGET
C2 beacon to known-bad domain	CRITICAL	10.0.0.5
Rogue device on LAN	HIGH	10.0.0.9
Exposed RDP service	HIGH	10.0.0.14

CISO NOTES

Prepared for the quarterly board risk review. Figures reconciled with Finance.