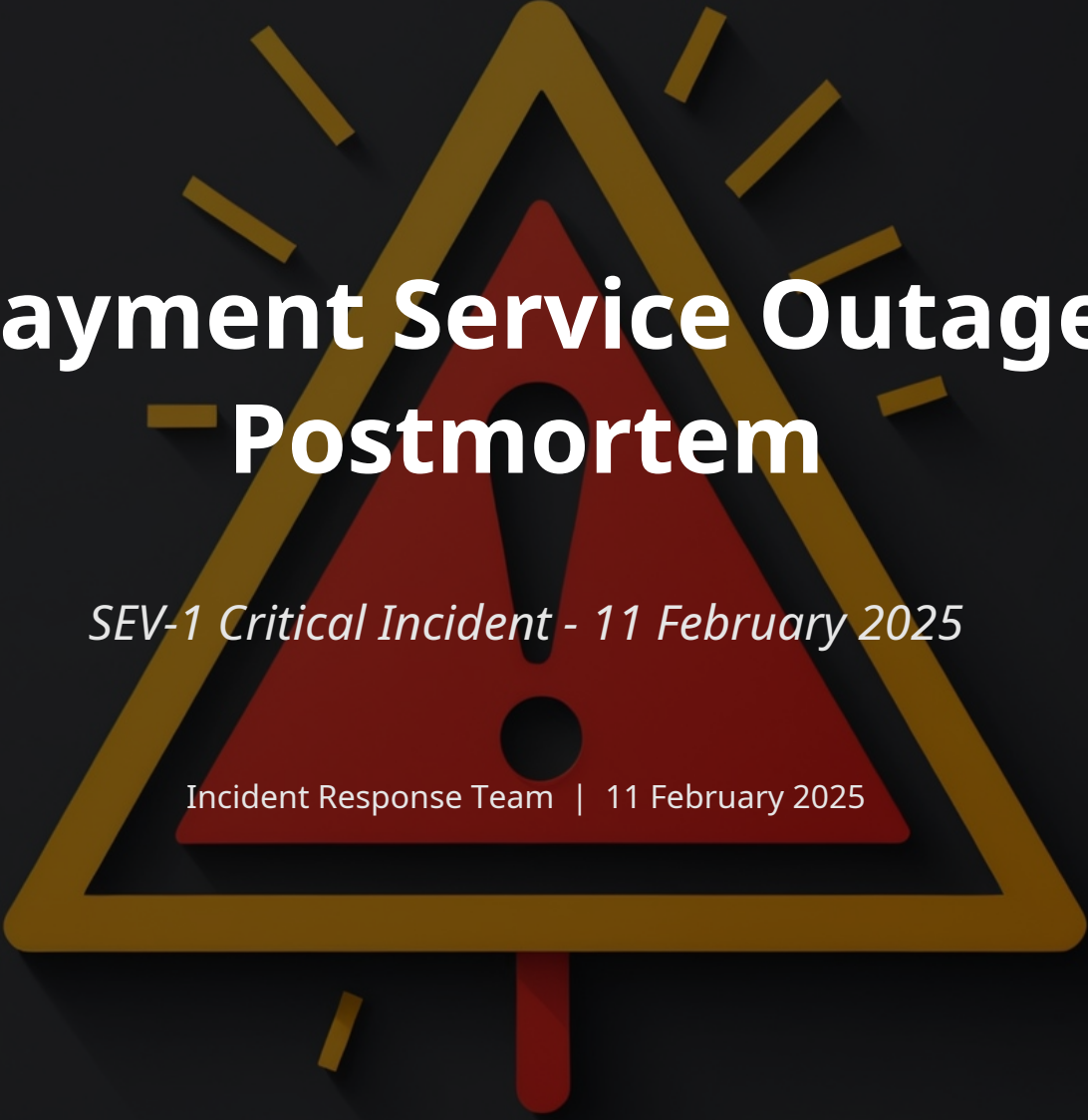


A large warning sign graphic is centered on the page. It features a red triangle with a black exclamation mark in the center. This triangle is enclosed within a larger, yellow-outlined triangle. Several short, yellow lines radiate from the top and sides of the yellow triangle, suggesting a bright light or a warning signal. The entire graphic is set against a dark gray background.

Payment Service Outage Postmortem

SEV-1 Critical Incident - 11 February 2025

Incident Response Team | 11 February 2025

Incident Summary

Severity	SEV-1 (Critical)
Incident Date	11 February 2025
Start Time	14:02 AEDT
End Time	16:49 AEDT
Total Duration	2h 47m
Systems Affected	payment-gateway, payment-api, checkout-service

Table 1: Incident Impact Summary

Metric	Value
Transactions Failed	62%
Customers Affected	18,400
Revenue Impact	\$146,000 AUD
Severity Level	SEV-1 (Critical)

Timeline of Events

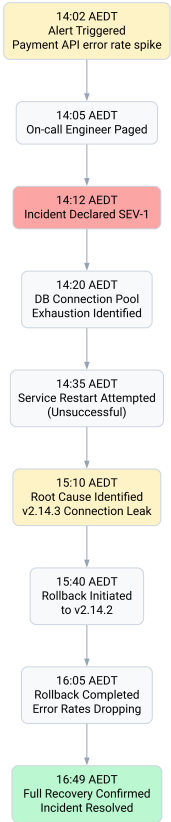


Figure 1: Incident Timeline (11 February 2025, AEDT)

The following timeline reconstructs the incident from initial alert through full recovery, all times shown in AEDT.

Key Timestamp & System Reference

14:02	payment-api	Error rate spike detected
14:05	pagerduty	On-call engineer paged
14:12	incident-mgmt	SEV-1 declared
14:20	payment-gateway	DB connection pool exhaustion identified
14:35	payment-gateway	Restart attempted (unsuccessful)
15:10	payment-gateway	Root cause identified: v2.14.3 leak
15:40	payment-gateway	Rollback initiated to v2.14.2
16:05	payment-gateway	Rollback completed
16:49	payment-api	Full recovery confirmed

Root Cause Analysis

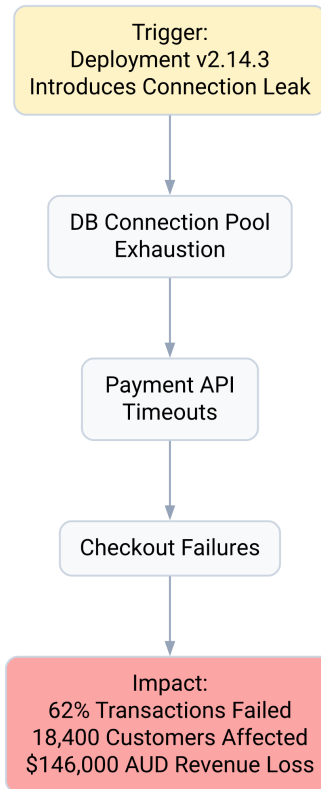


Figure 2: Failure Chain from Trigger to Impact

Root cause: Deployment of payment-gateway v2.14.3 introduced a database connection leak in the transaction-processing module.

This leak caused the connection pool to become exhausted under normal production load, which in turn caused payment-api requests to time out waiting for available connections.

Cascading timeouts propagated to checkout-service, resulting in widespread checkout failures and direct customer and revenue impact.

Resolution Steps Taken

- 1. Declared SEV-1 incident and paged the on-call engineering team.
- 2. Scaled up the database connection pool as a temporary mitigation.
- 3. Attempted a service restart of payment-gateway (unsuccessful).
- 4. Identified the faulty deployment via log and metric correlation.
- 5. Initiated rollback of payment-gateway to last known good version v2.14.2.
- 6. Validated error rates and transaction success rates post-rollback.
- 7. Monitored system stability for one hour before formally closing the incident.

Action Items & Owners

Table 2: Follow-up Action Items

Action Item	Owner	Due Date
Add automated DB connection pool leak detection	J. Tran (Platform Eng)	25 Feb 2025
Implement canary deployment gate for payment service	M. Silva (DevOps)	5 Mar 2025
Add pre-deploy load testing to CI pipeline	A. Kumar (QA)	10 Mar 2025
Update on-call runbook for DB pool exhaustion	L. Chen (SRE)	20 Feb 2025
Post-incident customer comms review	R. Patel (Support Lead)	18 Feb 2025

Lessons Learned

- Connection pool exhaustion was not caught by pre-deployment testing - load testing must simulate sustained production traffic patterns.
- The absence of a canary/staged rollout meant the faulty build reached 100% of production traffic immediately.
- Initial restart attempt delayed recovery; runbooks should prioritize rollback over restart when a recent deployment correlates with the incident onset.
- Cross-team communication during the incident was effective, but customer-facing comms lagged behind internal detection by nearly 20 minutes.
- Automated alerting on connection pool saturation would have surfaced the issue earlier, before customer impact began.