Incident Report

Incident Report

> **Project:** {{PROJECT_NAME}} **Version:** {{VERSION}} **Date:** {{DATE}}
> **Author:** {{AUTHOR}} **Status:** Draft | In Review | Approved **Reviewers:** {{REVIEWERS}}

Document History

Version	Date	Author	Changes
0.1	{{DATE}}	{{AUTHOR}}	Initial draft

---

1. Incident Metadata

Field	Value
Incident ID	INC-{{YYYY}}-{{SEQ}}
Severity	P{{SEVERITY}}
Status	{{STATUS}}
Incident Commander	{{IC}}
Technical Lead	{{TECH_LEAD}}
Communications Lead	{{COMMS_LEAD}}
Declared at	{{START_TIME}} {{TIMEZONE}}
Resolved at	{{END_TIME}} {{TIMEZONE}}
Total duration	{{DURATION}}
Affected service(s)	{{SERVICES}}
Environment	Production / Staging

---

2. Executive Summary

{{EXECUTIVE_SUMMARY}}

> Example: "On {{DATE}}, a database connection pool exhaustion caused the {{SERVICE}} API to return 503 errors for approximately 47 minutes, affecting {{AFFECTED_COUNT}} users and resulting in an estimated {{REVENUE_IMPACT}} in lost transactions. The root cause was a code change in the v{{VERSION}} deployment that introduced N+1 queries under high load."

---

3. Detection

Detected by: {{DETECTION_METHOD}} **Detected at:** {{DETECTION_TIME}} **Lag from start to detection:** {{DETECTION_LAG}} minutes **Detecting system:** {{DETECTING_SYSTEM}}

Alerting effectiveness:

- ☐ Alert fired within the expected window (< {{ALERT_SLA}} minutes)
- ☐ Alert delivered to on-call without delay
- ☐ Alert contained sufficient context to begin investigation

Improvements to detection identified:

- {{DETECTION_IMPROVEMENT_1}}

---

4. Detailed Timeline

> **Timezone:** All times in {{TIMEZONE}}

Time	Event	Actor	Notes
{{TIME}}	{{EVENT_1}}	{{ACTOR}}	
{{TIME}}	{{EVENT_2}}	System	Alert ID: {{ALERT_ID}}
{{TIME}}	{{EVENT_3}}	{{ENGINEER}}	

Time	Event	Actor	Notes
{{TIME}}	{{EVENT_4}}	{{IC}}	
{{TIME}}	{{EVENT_5}}	{{ENGINEER}}	
{{TIME}}	{{EVENT_6}}	{{ENGINEER}}	
{{TIME}}	{{EVENT_7}}	System	
{{TIME}}	{{EVENT_8}}	{{IC}}	

---

5. Impact Assessment

Users Affected

Metric	Value
Total users affected	{{USER_COUNT}}
% of total user base	{{USER_PERCENT}}%
Geography affected	{{GEOGRAPHY}}
User tier affected	{{USER_TIER}}

Services Affected

Service	Impact Type	Severity	Duration
{{SERVICE_1}}	{{IMPACT_TYPE}}	{{SEV}}	{{DURATION}}
{{SERVICE_2}}	{{IMPACT_TYPE}}	{{SEV}}	{{DURATION}}

Data Impact

Type	Assessment
Data loss	{{DATA_LOSS}}
Data corruption	{{DATA_CORRUPTION}}
Data exposure	{{DATA_EXPOSURE}}
Verification method	{{VERIFICATION}}

Financial Impact

Category	Amount	Notes
Lost transactions	${{AMOUNT}}	{{TRANSACTION_COUNT}} failed transactions
SLA credits	${{AMOUNT}}	Per SLA contract
Operational cost	${{AMOUNT}}	Engineering hours to resolve
Total estimated	**${{TOTAL}}**	

SLA Breach Assessment

SLA Metric	Target	Actual	Breach
Uptime	{{UPTIME_SLA}}%	{{ACTUAL_UPTIME}}%	{{BREACH}}
Response time (P99)	< {{P99_SLA}}ms	{{P99_ACTUAL}}ms	{{BREACH}}
MTTR	< {{MTTR_SLA}}	{{MTTR_ACTUAL}}	{{BREACH}}

---

6. Root Cause Analysis

5 Whys

Why #	Question	Answer
Why 1	Why did users see errors?	{{ANSWER_1}}
Why 2	Why was the API returning 503?	{{ANSWER_2}}
Why 3	Why was the connection pool exhausted?	{{ANSWER_3}}
Why 4	Why was the N+1 query introduced?	{{ANSWER_4}}
Why 5	Why did code review miss it?	{{ANSWER_5}}

Root cause: {{ROOT_CAUSE}}

Contributing Factors

1. {{FACTOR_1}}
2. {{FACTOR_2}}
3. {{FACTOR_3}}

Trigger Event

What triggered this specific incident now: {{TRIGGER}}

---

7. Resolution Steps

Step	Time	Action	Result
1	{{TIME}}	{{ACTION_1}}	{{RESULT_1}}
2	{{TIME}}	{{ACTION_2}}	{{RESULT_2}}
3	{{TIME}}	{{ACTION_3}}	{{RESULT_3}}

Resolution commands (for runbook):

```
# {{RESOLUTION_DESCRIPTION}}
{{RESOLUTION_COMMAND}}
```

---

8. What Went Well

1. {{WENT_WELL_1}}
2. {{WENT_WELL_2}}
3. {{WENT_WELL_3}}

---

9. What Went Wrong

1. {{WENT_WRONG_1}}
2. {{WENT_WRONG_2}}
3. {{WENT_WRONG_3}}

---

10. Action Items

#	Action	Owner	Due Date	Priority	Status
1	{{ACTION_1}}	{{OWNER}}	{{DUE}}	High	Open
2	{{ACTION_2}}	{{OWNER}}	{{DUE}}	High	Open
3	{{ACTION_3}}	{{OWNER}}	{{DUE}}	Medium	Open

#	Action	Owner	Due Date	Priority	Status
4	{{ACTION_4}}	{{OWNER}}	{{DUE}}	High	Open
5	{{ACTION_5}}	{{OWNER}}	{{DUE}}	Low	Open

11. Lessons Learned

1. {{LESSON_1}}
2. {{LESSON_2}}
3. {{LESSON_3}}

12. Related Incidents

Incident ID	Date	Similarity	Resolved
INC-{{ID}}	{{DATE}}	{{DESCRIPTION}}	Yes / No

13. Communication Log

Time	Channel	Message Summary	Audience	Sent By
{{TIME}}	Status page	"Investigating reports of elevated errors"	All users	{{SENDER}}
{{TIME}}	Status page	"Identified root cause, applying fix"	All users	{{SENDER}}
{{TIME}}	Status page	"Incident resolved, all systems normal"	All users	{{SENDER}}
{{TIME}}	Email	Customer notification for SLA breach	Affected customers	{{SENDER}}

Related Documents

- Post-Mortem
- Operational Runbook
- SLA Report

Approval

Role	Name	Date	Signature
Author			
Reviewer			
Approver			

Revision #6
Created 2026-02-23 12:06:14 UTC by John
Updated 2026-05-25 07:34:28 UTC by John