CHG0030015 — [TITAN] Critical — security on fw-allow-all-ingress

Severity	Critical	Priority	1 - Critical
Cloud	Multi	State	New
Resource	fw-allow-all-ingress	Group	network_operations
Resource type	compute.googleapis.com/Firewall	Change type	Normal
Opened	2026-04-21 15:26:56	Closed	2026-04-21 15:26:56
CAB required	Yes	Close code	—

Security Finding

```
GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to all VMs tagged
'default' — every GCE instance is publicly accessible over every port. Massive firewall
misconfiguration.
```

Justification

```
Severity assessment: CRITICAL — active exploit path, 0-day or internet-exposed asset. Meets ITIL
'security emergency' threshold.

Risk if deferred: Per industry telemetry, mean time to exploit a publicly-reachable
misconfiguration of this class is measured in hours. Delaying this change extends exposure window
and increases breach cost per IBM Cost of a Data Breach Report (avg $4.45M per incident).

Detected by: TITAN AI agent unknown (scan titan-killer-20260421T222654Z).
Finding: GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to all VMs
tagged 'default' — every GCE instance is publicly accessible over every port. Massive firewall
misconfiguration.
```

Implementation Plan

```
1. PRE-CHANGE VERIFICATION (5 min)
- Confirm TITAN pre-scan snapshot captured; snapshot ID in work notes.
- Confirm no blocking dependencies (check 'Affected CIs' below).
- Announce change start in #ops-change Slack channel.

2. APPLY FIX (primary command, auto-generated by TITAN):
gcloud compute firewall-rules update fw-allow-all-ingress
--source-ranges=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 --allowed=tcp:22,tcp:443

3. POST-CHANGE VERIFICATION (5 min)
- Re-run TITAN targeted scan on the affected resource.
- Confirm finding cleared (scan returns 0 matches for this finding_id).
- Smoke-test dependent applications (see Test plan).

4. CLOSE
- Update ticket state to Review -> Closed.
- Attach scan-diff evidence (pre vs post).
- If verification fails at step 3, execute Backout plan immediately.
```

Risk & Impact Analysis

Change risk level: HIGH (change risk: severity overrides defer-ability)

Blast radius: The change is scoped to a single cloud resource (GCP firewall rule 'fw-allow-all-ingress' allows any protocol from 0.0.0.0/0 to a...). Downstream dependencies (if any) are listed under 'Affected CIs'.

Applying this fix during business hours is acceptable given exploit exposure.

Worst-case failure mode: Change is rejected by the cloud API (network partition or permission drift). Impact: no state change on target resource; Backout plan is a no-op. Time to detect: immediate (non-zero exit code from fix command).

Residual risk after successful fix: zero — the finding no longer exists. TITAN verifies this via post-change scan (see Implementation plan step 3).

Backout / Rollback Plan

If post-change verification fails or the fix causes a service disruption:

1. IMMEDIATE: Revert the resource to its pre-change state using the TITAN pre-scan snapshot (snapshot ID recorded in work notes at scan time).
2. Azure: az <resource-type> update ... (inverse of the apply command) OR az deployment group create --template-uri <pre-change ARM URI>
3. AWS: aws <service> ... (restore from snapshot or inverse IAM policy)
4. GCP: gcloud <service> ... update --rollback
5. Confirm rollback succeeded by re-running TITAN scan — the original finding should reappear (confirming the state was fully reverted).
6. Document the failure mode in 'Close notes' for the post-incident review.
7. Re-open this change with 'Rejected' disposition and spawn a parent Problem ticket for root-cause analysis.

Test Plan

Acceptance criteria (must all PASS to close this change):

[ ] TITAN targeted re-scan of GCP firewall rule 'fw-allow-all-ingress' allows any protocol... returns ZERO matches for this finding_id.
[ ] Resource remains in provisioning_state=Succeeded (Azure) / available (AWS) / RUNNING (GCP) immediately after change.
[ ] Dependent applications pass smoke tests (HTTP 200 on health endpoints, auth still works for service accounts, DB connection-strings unchanged).
[ ] No new alerts raised in Azure Monitor / CloudWatch / Cloud Monitoring in the 30 minutes following the change.
[ ] Audit chain entry written: agent.change.applied event with pre/post hashes.

Any FAIL triggers the Backout plan above. Evidence attached to 'Closure Information' tab.

Recommended Fix Command

```
gcloud compute firewall-rules update fw-allow-all-ingress
--source-ranges=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 --allowed=tcp:22,tcp:443
```

Compliance Mapping

CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, CIS Azure 6.2

AI Close Notes

(empty)