OWASP MCP Top 10

Compliance assessment — 2025

Server: compute.googleapis.com

Slug: compute-googleapis-com-20260728163042-10277d
Scan id: 39b117c1-9a86-4b15-bc6d-f467555c73b6

Assessed at: 2026-07-28 16:30:43 UTC
Sentinel version: 0.4.0
Rules version: 2026-04-23

' Non-compliant

DRAFT for review — not legal advice. See attestation block for verification instructions.

DRAFT

Table of contents

1. Executive summary
2. Coverage & transparency
3. Controls summary
4. Control details
5. Multi-step attack chains
6. Cryptographic attestation

1. Executive summary

Assessment of compute.googleapis.com against OWASP MCP Top 10: overall status non compliant. Of 10 controls, 0 met, 1 unmet, 1 partial, 8 not assessed, 0 not applicable. 2 control(s) had complete mapped-assessor execution evidence; 8 lacked sufficient execution evidence and 0 were outside the current assessor mapping. Unmet controls have findings at or above the framework's mandatory severity threshold and should be remediated before relying on this server in a regulated deployment. All claims are traceable to individual finding rows via finding_id and to the governing rule via rule_id; the enclosing signed envelope commits MCP Sentinel to the exact bytes of this report.

2. Coverage & transparency

Coverage band: low

Coverage ratio: 32%

Rules version: 2026-04-23

Analysis techniques applied:

- capability-graph
- composite
- linguistic
- schema-inference
- similarity
- structural
- stub
- unicode

3. Controls summary

ControlName	Status	Evidence
MCP01Prompt Injection?	Not	

assessed0
MCP02Tool Poisoning' Unmet1
MCP03 Command Injection? Not assessed0
MCP04Data Exfiltration? Not assessed0
MCP05 Privilege Escalation? Not assessed0
MCP06 Excessive Permissions? Not assessed0
MCP07 Insecure Configuration! Partial30
MCP08 Dependency Vulnerabilities ? Not assessed0
MCP09 Logging & Monitoring Failures? Not assessed0
MCP10Supply Chain Compromise? Not assessed0

4. Control details

MCP01 — Prompt Injection

? Not assessed

0/24 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A1 (execution-ledger); A5 (execution-ledger); A7 (execution-ledger); A8 (execution-ledger); A9 (execution-ledger); B5 (execution-ledger); F1 (execution-ledger); F6 (execution-ledger); G1 (execution-ledger); G2 (execution-ledger); G3 (execution-ledger); G4 (execution-ledger); G5 (execution-ledger); H2 (execution-ledger); H3 (execution-ledger); I3 (execution-ledger); I6 (execution-ledger); I7 (execution-ledger); J3 (execution-ledger); J5 (execution-ledger); J6 (execution-ledger); N4 (execution-ledger); N9 (execution-ledger); N12 (execution-ledger).

MCP02 — Tool Poisoning

' Unmet

0/15 mapped assessor rule(s) are proven to have executed; 1 finding(s) observed (1 critical); at least one finding is at or above the high threshold (status: unmet). 15 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[Critical] Tool Annotation Deception (finding f9eb7e57-7328-476c-a971-e30f5b5f9faa, confidence 85%)

SOURCE: external-content at tool list_instance_attached_disks — The MCP spec (2025-03-26) treats tool annotations as server-declared hints that AI clients may use to skip user confirmation. readOnlyHi

Required mitigations:

- Remove readOnlyHint: true from any tool whose parameters or description indicate write, delete, or overwrite capability. If the tool is genuinely read-only, rename the misleading parameter or update the description. If the tool is destructive, set destructiveHint: true so AI clients require user confirmation before invocation. AI clients (ChatGPT, Cursor, Roo Code, JetBrains Copilot per Invariant Labs 2025) auto-approve tools declaring readOnlyHint: true without cross-checking the schema — a deceptive annotation bypasses the strongest consent control in the MCP protocol.

MCP03 — Command Injection

? Not assessed

0/6 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: C1 (execution-ledger); C9 (execution-ledger); C13 (execution-ledger); C16 (execution-ledger); J2 (execution-ledger); J7 (execution-ledger).

MCP04 — Data Exfiltration

? Not assessed

0/15 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A3 (execution-ledger); F1 (execution-ledger); F3 (execution-ledger); F7 (execution-ledger); G7 (execution-ledger); I9 (execution-ledger); I13 (execution-ledger); K18 (execution-ledger); O4 (execution-ledger); O5 (execution-ledger); O6 (execution-ledger); O8 (execution-ledger); O9 (execution-ledger); O10 (execution-ledger); P3 (execution-ledger).

MCP05 — Privilege Escalation

? Not assessed

0/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: C2 (execution-ledger); C8 (execution-ledger); C10 (execution-ledger); C12 (execution-ledger); I4 (execution-ledger); I12 (execution-ledger); J1 (execution-ledger).

MCP06 — Excessive Permissions

? Not assessed

0/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A2 (execution-ledger); B3 (execution-ledger); B7 (execution-ledger); E4 (execution-ledger); F2 (execution-ledger); I11 (execution-ledger); I16 (execution-ledger).

MCP07 — Insecure Configuration

! Partial

0/11 mapped assessor rule(s) are proven to have executed; 30 finding(s) observed (30 medium); all findings are below the high threshold (status: partial). 11 mapped assessor(s) did not execute, so this finding-backed result does not imply complete control coverage.

Evidence:

[Medium] Schema Allows Unconstrained Additional Properties (finding e5dd1b89-57b6-41b8-890b-b3f08a5c9744, confidence 75%)

SOURCE: user-parameter at tool create_instance — Tool "create_instance" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that

[Medium] Schema Allows Unconstrained Additional Properties (finding cca23fe0-7b1f-4e3a-a238-f8f990ab2cda, confidence 75%)

SOURCE: user-parameter at tool delete_instance — Tool "delete_instance" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that

[Medium] Schema Allows Unconstrained Additional Properties (finding 4713c590-66a3-4dfc-9532-c6b7559fd67a, confidence 75%)

SOURCE: user-parameter at tool start_instance — Tool "start_instance" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that by

[Medium] Schema Allows Unconstrained Additional Properties (finding 8bc1f684-a322-408c-845f-81e109781d8d, confidence 75%)

SOURCE: user-parameter at tool stop_instance — Tool "stop_instance" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that bypa

[Medium] Schema Allows Unconstrained Additional Properties (finding 6f40d60c-b25b-4bb4-a6aa-

9bd8dd56b1ef,
confidence 75%)
SOURCE: user-parameter at tool reset_instance — Tool "reset_instance" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that by
[Medium]
Schema Allows
Unconstrained
Additional
Properties
(finding a9ca73fd
-9375-439d-92db
-2e7d784186b2,
confidence 75%)
SOURCE: user-parameter at tool get_instance_basic_info — Tool "get_instance_basic_info" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undec
[Medium]
Schema Allows
Unconstrained
Additional
Properties
(finding b10266fa
-5957-4c41-9d8d
-74c0f7472043,
confidence 75%)
SOURCE: user-parameter at tool set_instance_machine_type — Tool "set_instance_machine_type" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read u
[Medium]
Schema Allows
Unconstrained
Additional
Properties
(finding 51b4f92c
-3a9d-4a6f-a89c-
11a22432e857,
confidence 75%)
SOURCE: user-parameter at tool list_instance_attached_disks — Tool "list_instance_attached_disks" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may
[Medium]
Schema Allows
Unconstrained
Additional
Properties
(finding
98a4089c-
f97c-4e08-a53e-
309184fcb8d6,
confidence 75%)
SOURCE: user-parameter at tool list_instances — Tool "list_instances" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that by
[Medium]
Schema Allows
Unconstrained
Additional
Properties
(finding
592ee716-
fdcc-4019-bac6-
ca6335c74ec0,
confidence 75%)
SOURCE: user-parameter at tool get_instance_group_manager_basic_info — Tool "get_instance_group_manager_basic_info" input_schema accepts arbitrary extra keys. The declared properties

are validated, bu

[Medium]

Schema Allows Unconstrained Additional Properties (finding 117ff4d0-a119-4f6b-8c83-bf7d7cf68a53, confidence 75%)

SOURCE: user-parameter at tool list_instance_group_managers — Tool "list_instance_group_managers" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may

[Medium]

Schema Allows Unconstrained Additional Properties (finding a9eb034b-403e-47a3-a05a-e3ade9c9c9e8, confidence 75%)

SOURCE: user-parameter at tool list_managed_instances — Tool "list_managed_instances" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undecla

[Medium]

Schema Allows Unconstrained Additional Properties (finding ba57e051-28c3-478f-a3b2-2762b822c9e5, confidence 75%)

SOURCE: user-parameter at tool list_instance_templates — Tool "list_instance_templates" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undec

[Medium]

Schema Allows Unconstrained Additional Properties (finding b12906bf-c95e-4b92-b8f5-57b21c30c9a2, confidence 75%)

SOURCE: user-parameter at tool get_instance_template_basic_info — Tool "get_instance_template_basic_info" input_schema accepts arbitrary extra keys. The declared properties are validated, but the hand

[Medium]

Schema Allows Unconstrained Additional Properties (finding 34e25997-f84d-4124-991e-7233265db93a, confidence 75%)

SOURCE: user-parameter at tool get_instance_template_properties — Tool

"get_instance_template_properties" input_schema accepts arbitrary extra keys. The declared properties are validated, but the hand

[Medium]
Schema Allows Unconstrained Additional Properties (finding 22cd2e9a-e75e-45a5-a6a4-4adef5316948, confidence 75%)
SOURCE: user-parameter at tool get_disk_basic_info — Tool "get_disk_basic_info" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared ke

[Medium]
Schema Allows Unconstrained Additional Properties (finding 444b65a1-2a28-4916-b55b-b7084744ad02, confidence 75%)
SOURCE: user-parameter at tool get_disk_performance_config — Tool "get_disk_performance_config" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may re

[Medium]
Schema Allows Unconstrained Additional Properties (finding 65d2b5d7-9a77-407e-bd6f-5d20e51617d2, confidence 75%)
SOURCE: user-parameter at tool list_disks — Tool "list_disks" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that bypass eve

[Medium]
Schema Allows Unconstrained Additional Properties (finding 0769aee4-219b-4d9c-bf4d-99ea8db55d57, confidence 75%)
SOURCE: user-parameter at tool list_accelerator_types — Tool "list_accelerator_types" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undecla

[Medium]
Schema Allows Unconstrained Additional Properties (finding 3be2bbe4-e85a-4fac-a4d0-bd34e989d7c7, confidence 75%)
SOURCE: user-parameter at tool list_machine_types — Tool "list_machine_types" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys

[Medium]
Schema Allows Unconstrained Additional Properties (finding 2c65db68-2026-49f1-a6a7-c58281d6d6dd, confidence 75%)
SOURCE: user-parameter at tool list_images — Tool "list_images" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that bypass e

[Medium]
Schema Allows Unconstrained Additional Properties (finding 52c52d69-5d6d-40c5-8465-964fc467aaa8, confidence 75%)
SOURCE: user-parameter at tool get_zone_operation — Tool "get_zone_operation" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys

[Medium]
Schema Allows Unconstrained Additional Properties (finding 1ae01d30-5637-45c0-8a47-a7238d99e9fc, confidence 75%)
SOURCE: user-parameter at tool get_reservation_basic_info — Tool "get_reservation_basic_info" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read

[Medium]
Schema Allows Unconstrained Additional Properties (finding d5e9ab90-d6f3-42cd-acce-194b33a117fc, confidence 75%)
SOURCE: user-parameter at tool get_reservation_details — Tool "get_reservation_details" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undec

[Medium]
Schema Allows Unconstrained Additional Properties (finding fe5ac821-00f7-4f03-b993-8e01d8662b57, confidence 75%)
SOURCE: user-parameter at tool list_reservations — Tool "list_reservations" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys t

[Medium]
Schema Allows Unconstrained Additional

Properties (finding 2db588c0-713f-4c07-a305-1b91ac7d3370, confidence 75%)
SOURCE: user-parameter at tool list_commitments — Tool "list_commitments" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys tha
[Medium] Schema Allows Unconstrained Additional Properties (finding 762d401f-48c7-4b82-8660-331775c01491, confidence 75%)
SOURCE: user-parameter at tool get_commitment_basic_info — Tool "get_commitment_basic_info" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read u
[Medium] Schema Allows Unconstrained Additional Properties (finding ebd36c86-f290-47ad-9170-57800c5476ca, confidence 75%)
SOURCE: user-parameter at tool list_commitment_reservations — Tool "list_commitment_reservations" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may
[Medium] Schema Allows Unconstrained Additional Properties (finding 4c303000-030e-48ab-9d25-b7e59b0832a6, confidence 75%)
SOURCE: user-parameter at tool list_snapshots — Tool "list_snapshots" input_schema accepts arbitrary extra keys. The declared properties are validated, but the handler may read undeclared keys that by
[Medium] No Authentication Required (finding 845971fb-be88-4217-9ce3-43fcf7983964, confidence 75%)
SOURCE: environment at capability:tools — An MCP server that answers tool enumeration without authentication trusts the network. Under modern threat models (CCS 2007 DNS rebinding, open cloud networki

Required mitigations:

- Set additionalProperties: false on every object schema. This rejects any key outside the declared properties, closing the side-channel smuggling path and enforcing the schema's stated contract.
- Require authentication for all MCP server connections. For remote MCP servers adopt OAuth 2.0 per RFC 9700 / the MCP Authorization specification. For stdio-launched servers rely on the parent process's security boundary and DO NOT expose the same server over network transports. Even localhost-bound servers should require auth: DNS rebinding (CCS 2007) makes localhost reachable

from any browser tab.

MCP08 — Dependency Vulnerabilities

? Not assessed

0/7 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: D1 (execution-ledger); D2 (execution-ledger); D3 (execution-ledger); D4 (execution-ledger); D5 (execution-ledger); D6 (execution-ledger); D7 (execution-ledger).

MCP09 — Logging & Monitoring Failures

? Not assessed

0/6 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: C6 (execution-ledger); E3 (execution-ledger); K1 (execution-ledger); K2 (execution-ledger); K3 (execution-ledger); K20 (execution-ledger).

MCP10 — Supply Chain Compromise

? Not assessed

0/27 mapped assessor rule(s) are proven to have executed; no adverse findings were observed, but the control is not assessed because execution evidence is incomplete. Unexecuted assessors: A4 (execution-ledger); D3 (execution-ledger); D5 (execution-ledger); D7 (execution-ledger); F5 (execution-ledger); I5 (execution-ledger); J7 (execution-ledger); K9 (execution-ledger); K10 (execution-ledger); K11 (execution-ledger); L1 (execution-ledger); L2 (execution-ledger); L3 (execution-ledger); L4 (execution-ledger); L5 (execution-ledger); L6 (execution-ledger); L7 (execution-ledger); L8 (execution-ledger); L9 (execution-ledger); L10 (execution-ledger); L11 (execution-ledger); L12 (execution-ledger); L13 (execution-ledger); L14 (execution-ledger); L15 (execution-ledger); Q4 (execution-ledger); Q13 (execution-ledger).

5. Multi-step attack chains

No multi-step attack chains were synthesized for this server.

6. Cryptographic attestation

Algorithm: `HMAC-SHA256`
Key ID: `mcps-hkdf-e8990a4e1526`
Signer: `mcp-sentinel/v1`
Signed at: `2026-07-28T16:30:43.290Z`
Canonicalization: RFC8785

HMAC-SHA256 signature (base64, wrapped at 64 chars):

```
Xs4Ru3BGA7RXfxRposcJZ9+O69c+7hRlJm0rOT/FeYs=
```

Verification instructions:

```
To verify this report:
  1. Extract the report body (everything except the .attestation field).
  2. Canonicalize the body via RFC 8785 (JCS).
  3. Compute HMAC-SHA256 with the signing key for key_id "mcps-hkdf-e8990a4e1526".
  4. Base64-encode the result and compare with the signature above.
```