



# MCP Registry: OCI ownership validation fails open on upstream rate limits, allowing attacker-controlled package claims

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-45781
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-14 21:16:48 UTC
<b>Updated</b>	2026-05-14 21:16:48 UTC
<b>Description</b>	The MCP Registry provides MCP clients with a list of MCP servers, like an app store for MCP servers. Prior to 1.7.9, OCI o

## Risk And Classification

**Primary CVSS:** v3.1 3.5 LOW from security-advisories@github.com

**CVSS:** 3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N

**Problem Types:** CWE-636 | CWE-636 CWE-636: Not Failing Securely ('Failing Open')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Modelcontextprotocol</a>	<a href="#">Registry</a>	affected < 1.7.9	Not specified

### References

Reference	Source	Link	Tags
<a href="https://github.com/modelcontextprotocol/registry/security/advisories/GHSA-2v5f-5...">github.com/modelcontextprotocol/registry/security/advisories/GHSA-2v5f-5...</a>	<a href="mailto:security-advisories@github.com">security-advisories@github.com</a>	<a href="https://github.com">github.com</a>	
CVE Program record	<a href="https://www.cve.org">CVE.ORG</a>	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	<a href="https://nvd.nist.gov">NVD</a>	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)