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

CVE	CVE-2026-45781
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 21:16:48 UTC
Updated	2026-05-14 21:16:48 UTC
Description	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	Modelcontextprotocol	Registry	affected < 1.7.9	Not specified

References

Reference	Source	Link	Tags
github.com/modelcontextprotocol/registry/security/advisories/GHSA-2v5f-5...	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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