



AgiFlow scaffold-mcp write-to-file Tool index.ts path traversal

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

Summary

CVE	CVE-2026-7237
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 08:16:02 UTC
Updated	2026-04-28 08:16:02 UTC
Description	A vulnerability was detected in AgiFlow scaffold-mcp up to 1.0.27. Affected by this issue is some unknown functionality of t

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-22 | CWE-22 Path Traversal

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	AgiFlow	Scaffold-mcp	affected 1.0.0	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.1	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.2	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.3	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.4	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.5	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.6	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.7	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.8	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.9	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.10	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.11	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.12	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.13	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.14	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.15	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.16	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.17	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.18	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.19	Not specified
CNA	AgiFlow	Scaffold-mcp	affected 1.0.20	Not specified

CNA	Agiflow	Scaffold-mcp	affected 1.0.21	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.21	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.22	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.23	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.24	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.25	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.26	Not specified
CNA	Agiflow	Scaffold-mcp	affected 1.0.27	Not specified
CNA	Agiflow	Scaffold-mcp	unaffected 1.1.0	Not specified

References

Reference	Source	Link	Tags
github.com/Agiflow/aicode-toolkit/pull/89	cna@vuldb.com	github.com	
github.com/Agiflow/aicode-toolkit/issues/88	cna@vuldb.com	github.com	
vuldb.com/submit/802836	cna@vuldb.com	vuldb.com	
github.com/Agiflow/aicode-toolkit/commit/c4d23592ae5fb59cfeefc4641e6826f...	cna@vuldb.com	github.com	
github.com/Agiflow/aicode-toolkit/releases/tag/%40agiflowai/aicode-toolk...	cna@vuldb.com	github.com	
vuldb.com/vuln/359845	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/359845/cti	cna@vuldb.com	vuldb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: BruceJin (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-27T00:00:00.000Z	Advisory disclosed
CNA	2026-04-27T02:00:00.000Z	VulDB entry created
CNA	2026-04-27T19:22:42.000Z	VulDB entry last update

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

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

CVE.report and Source URL Uptime Status status.cve.report