vercel ai provider-utils response-handler.ts createJsonErrorResponseHandler resource consumption

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-8769
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-17 23:17:03 UTC
Updated	2026-05-17 23:17:03 UTC
Description	A vulnerability was determined in vercel ai up to 3.0.97. The impacted element is the function createJsonResponseHandler/

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-400 | CWE-404 | CWE-400 Resource Consumption | CWE-404 Denial of Service

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	4.3	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	4		AV:N/AC:L/Au:S/C:N/I:N/A:P
2.0	CNA	DECLARED	4		AV:N/AC:L/Au:S/C:N/I:N/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

None

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/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/MSC: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

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vercel	Ai	affected 3.0.0	Not specified
CNA	Vercel	Ai	affected 3.0.1	Not specified
CNA	Vercel	Ai	affected 3.0.2	Not specified
CNA	Vercel	Ai	affected 3.0.3	Not specified
CNA	Vercel	Ai	affected 3.0.4	Not specified
CNA	Vercel	Ai	affected 3.0.5	Not specified
CNA	Vercel	Ai	affected 3.0.6	Not specified
CNA	Vercel	Ai	affected 3.0.7	Not specified
CNA	Vercel	Ai	affected 3.0.8	Not specified
CNA	Vercel	Ai	affected 3.0.9	Not specified
CNA	Vercel	Ai	affected 3.0.10	Not specified
CNA	Vercel	Ai	affected 3.0.11	Not specified
CNA	Vercel	Ai	affected 3.0.12	Not specified
CNA	Vercel	Ai	affected 3.0.13	Not specified
CNA	Vercel	Ai	affected 3.0.14	Not specified
CNA	Vercel	Ai	affected 3.0.15	Not specified
CNA	Vercel	Ai	affected 3.0.16	Not specified
CNA	Vercel	Ai	affected 3.0.17	Not specified
CNA	Vercel	Ai	affected 3.0.18	Not specified

CNA	Vercel	Ai	affected 3.0.19	Not specified
CNA	Vercel	Ai	affected 3.0.20	Not specified
CNA	Vercel	Ai	affected 3.0.21	Not specified
CNA	Vercel	Ai	affected 3.0.22	Not specified
CNA	Vercel	Ai	affected 3.0.23	Not specified
CNA	Vercel	Ai	affected 3.0.24	Not specified
CNA	Vercel	Ai	affected 3.0.25	Not specified
CNA	Vercel	Ai	affected 3.0.26	Not specified
CNA	Vercel	Ai	affected 3.0.27	Not specified
CNA	Vercel	Ai	affected 3.0.28	Not specified
CNA	Vercel	Ai	affected 3.0.29	Not specified
CNA	Vercel	Ai	affected 3.0.30	Not specified
CNA	Vercel	Ai	affected 3.0.31	Not specified
CNA	Vercel	Ai	affected 3.0.32	Not specified
CNA	Vercel	Ai	affected 3.0.33	Not specified
CNA	Vercel	Ai	affected 3.0.34	Not specified
CNA	Vercel	Ai	affected 3.0.35	Not specified
CNA	Vercel	Ai	affected 3.0.36	Not specified
CNA	Vercel	Ai	affected 3.0.37	Not specified
CNA	Vercel	Ai	affected 3.0.38	Not specified
CNA	Vercel	Ai	affected 3.0.39	Not specified
CNA	Vercel	Ai	affected 3.0.40	Not specified
CNA	Vercel	Ai	affected 3.0.41	Not specified
CNA	Vercel	Ai	affected 3.0.42	Not specified
CNA	Vercel	Ai	affected 3.0.43	Not specified
CNA	Vercel	Ai	affected 3.0.44	Not specified
CNA	Vercel	Ai	affected 3.0.45	Not specified
CNA	Vercel	Ai	affected 3.0.46	Not specified
CNA	Vercel	Ai	affected 3.0.47	Not specified
CNA	Vercel	Ai	affected 3.0.48	Not specified
CNA	Vercel	Ai	affected 3.0.49	Not specified
CNA	Vercel	Ai	affected 3.0.50	Not specified
CNA	Vercel	Ai	affected 3.0.51	Not specified
CNA	Vercel	Ai	affected 3.0.52	Not specified
CNA	Vercel	Ai	affected 3.0.53	Not specified

CNA	Vercel	Ai	affected 3.0.54	Not specified
CNA	Vercel	Ai	affected 3.0.55	Not specified
CNA	Vercel	Ai	affected 3.0.56	Not specified
CNA	Vercel	Ai	affected 3.0.57	Not specified
CNA	Vercel	Ai	affected 3.0.58	Not specified
CNA	Vercel	Ai	affected 3.0.59	Not specified
CNA	Vercel	Ai	affected 3.0.60	Not specified
CNA	Vercel	Ai	affected 3.0.61	Not specified
CNA	Vercel	Ai	affected 3.0.62	Not specified
CNA	Vercel	Ai	affected 3.0.63	Not specified
CNA	Vercel	Ai	affected 3.0.64	Not specified
CNA	Vercel	Ai	affected 3.0.65	Not specified
CNA	Vercel	Ai	affected 3.0.66	Not specified
CNA	Vercel	Ai	affected 3.0.67	Not specified
CNA	Vercel	Ai	affected 3.0.68	Not specified
CNA	Vercel	Ai	affected 3.0.69	Not specified
CNA	Vercel	Ai	affected 3.0.70	Not specified
CNA	Vercel	Ai	affected 3.0.71	Not specified
CNA	Vercel	Ai	affected 3.0.72	Not specified
CNA	Vercel	Ai	affected 3.0.73	Not specified
CNA	Vercel	Ai	affected 3.0.74	Not specified
CNA	Vercel	Ai	affected 3.0.75	Not specified
CNA	Vercel	Ai	affected 3.0.76	Not specified
CNA	Vercel	Ai	affected 3.0.77	Not specified
CNA	Vercel	Ai	affected 3.0.78	Not specified
CNA	Vercel	Ai	affected 3.0.79	Not specified
CNA	Vercel	Ai	affected 3.0.80	Not specified
CNA	Vercel	Ai	affected 3.0.81	Not specified
CNA	Vercel	Ai	affected 3.0.82	Not specified
CNA	Vercel	Ai	affected 3.0.83	Not specified
CNA	Vercel	Ai	affected 3.0.84	Not specified
CNA	Vercel	Ai	affected 3.0.85	Not specified
CNA	Vercel	Ai	affected 3.0.86	Not specified
CNA	Vercel	Ai	affected 3.0.87	Not specified
CNA	Vercel	Ai	affected 3.0.88	Not specified
CNA	Vercel	Ai	affected 3.0.89	Not specified

CNA	Vercel	Ai	affected 3.0.89	Not specified
CNA	Vercel	Ai	affected 3.0.90	Not specified
CNA	Vercel	Ai	affected 3.0.91	Not specified
CNA	Vercel	Ai	affected 3.0.92	Not specified
CNA	Vercel	Ai	affected 3.0.93	Not specified
CNA	Vercel	Ai	affected 3.0.94	Not specified
CNA	Vercel	Ai	affected 3.0.95	Not specified
CNA	Vercel	Ai	affected 3.0.96	Not specified
CNA	Vercel	Ai	affected 3.0.97	Not specified

References

Reference	Source	Link	Tags
vuldb.com/submit/811406	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/364394/cti	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/364394	cna@vuldb.com	vuldb.com	
gist.github.com/YLChen-007/fb1096bc8428bed9a428f764d9d103bb	cna@vuldb.com	gist.github.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: Eric-f (VulDB User) (en)

CNA: VulDB CNA Team (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-05-17T00:00:00.000Z	Advisory disclosed
CNA	2026-05-17T02:00:00.000Z	VulDB entry created
CNA	2026-05-17T11:33:28.000Z	VulDB entry last update

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

Free CVE JSON API cve.report/api

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