



Sinaptik AI PandasAI sql_sanitizer.py is_sql_query_safe path traversal

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-4997 |
| State | PUBLISHED |
| Assigner | VulDB |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-28 13:16:34 UTC |
| Updated | 2026-03-30 13:26:07 UTC |
| Description | A security flaw has been discovered in Sinaptik AI PandasAI up to 3.0.0. This affects the function is_sql_query_safe of the 1 |

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from cna@vuldb.com

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

EPSS: 0.000570000 probability, percentile 0.178690000 (date 2026-04-02)

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

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------|-----------|-------|----------|---|
| 4.0 | cna@vuldb.com | Secondary | 5.5 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P/C.. |
| 4.0 | CNA | DECLARED | 6.9 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:P |
| 3.1 | cna@vuldb.com | Primary | 5.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| 3.1 | CNA | DECLARED | 5.3 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R |
| 3.0 | CNA | DECLARED | 5.3 | MEDIUM | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:X/RC:R |
| 2.0 | cna@vuldb.com | Secondary | 5 | | AV:N/AC:L/Au:N/C:P/I:N/A:N |
| 2.0 | CNA | DECLARED | 5 | | AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POG/RL:ND/RC:UR |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

None

Availability

None

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:N/VA:N/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

CVSS v3.0 Breakdown

Attack Vector

Network

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|-------------|----------|--------------|---------------|
| CNA | Sinaptik AI | PandasAI | affected 3.0 | Not specified |

References

| Reference | Source | Link | Tags |
|---|---------------|-----------------|---------------------|
| vuldb.com/submit/778269 | cna@vuldb.com | vuldb.com | |
| vuldb.com/vuln/353884 | cna@vuldb.com | vuldb.com | |
| vuldb.com/vuln/353884/cti | cna@vuldb.com | vuldb.com | |
| gist.github.com/YLChen-007/0ea2685789929bdb6363f5aebb7cba9a | 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-b (VulDB User) (en)

CNA: VulDB (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|---------------------|
| CNA | 2026-03-27T00:00:00.000Z | Advisory disclosed |
| CNA | 2026-03-27T01:00:00.000Z | VulDB entry created |

CNA

2026-03-27T14:53:52.000Z

VulDB entry last update

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)