



Improper neutralization of input during web page generation vulnerability has been discovered in OpenText™ Vertica.

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2025-12453 |
| State | PUBLISHED |
| Assigner | OpenText |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-13 19:53:47 UTC |
| Updated | 2026-04-17 15:25:00 UTC |
| Description | Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in OpenText™ Vertica allow |

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from security@opentext.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/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:Y/R:U/V:X/RE:X/U:X

EPSS: 0.000350000 probability, percentile 0.105050000 (date 2026-04-21)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

| Version | Source | Type | Score | Severity | Vector |
|---------|-----------------------|-----------|-------|----------|---|
| 4.0 | security@opentext.com | Secondary | 5.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E |
| 4.0 | CNA | CVSS | 5.1 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/A |
| 3.1 | nvd@nist.gov | Primary | 6.1 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N/E:X/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:Y/R:U/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|---------|---------|--------|---------|----------|
| Application | Opentext | Vertica | All | All | All | All |

Vendor Declared Affected Products

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|--------------------------|-------------------------|-------------------------------|---------------|
| CNA | OpenText | Vertica | affected 10.0 10.x custom | Not specified |
| CNA | OpenText | Vertica | affected 11.0 11.x custom | Not specified |
| CNA | OpenText | Vertica | affected 12.0 12.x custom | Not specified |
| CNA | OpenText | Vertica | affected 23.0 23.x custom | Not specified |
| CNA | OpenText | Vertica | affected 24.0 24.x custom | Not specified |
| CNA | OpenText | Vertica | affected 25.1.0 25.1.x custom | Not specified |
| CNA | OpenText | Vertica | affected 25.2.0 25.2.x custom | Not specified |
| CNA | OpenText | Vertica | affected 25.3.0 25.3.x custom | Not specified |

References

| Reference | Source | Link | Tags |
|---|--|---|---------------------|
| portal.microfocus.com/s/article/KM000045852 | security@opentext.com | portal.microfocus.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: https://portal.microfocus.com/s/article/KM000045852?language=en_US

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

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