



# Pega Platform versions 8.1.0 through 25.1.1 are affected by an HTML Injection vulnerability in a user interface component. Requires a high privileged user with a developer role.

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-1564
<b>State</b>	PUBLISHED
<b>Assigner</b>	Pega
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-15 22:16:51 UTC
<b>Updated</b>	2026-04-17 15:38:09 UTC
<b>Description</b>	Pega Platform versions 8.1.0 through 25.1.1 are affected by an HTML Injection vulnerability in a user interface component.

## Risk And Classification

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

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

**EPSS:** 0.000570000 probability, percentile 0.177420000 (date 2026-04-21)

**Problem Types:** CWE-80 | CWE-80 CWE-80: Improper Neutralization of Script Related HTML Tags in a Web Page

Version	Source	Type	Score	Severity	Vector
4.0	security@pega.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:N/SC:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Attack Requirements

**None**

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pegasystems	Pega Infinity	affected 8.1.0 Infinity 25.1.2 custom	Not specified

### References

Reference	Source	Link	Tags
support.pega.com/support-doc/pega-security-advisory-b26-vulnerability-remediat...	security@pega.com	<a href="https://support.pega.com">support.pega.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, an

### Vendor Comments And Credit

Discovery Credit

**CNA:** Michal Skowron from ING Hubs Poland (en)

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)