



Pega Platform versions 8.1.0 through 25.1.1 are affected by a Stored Cross-Site Scripting vulnerability in a user interface component. Requires a high privileged user with a developer role.

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-1711 |
| State | PUBLISHED |
| Assigner | Pega |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-04-15 22:16:51 UTC |
| Updated | 2026-04-23 20:01:09 UTC |
| Description | Pega Platform versions 8.1.0 through 25.1.1 are affected by a Stored Cross-Site Scripting vulnerability in a user interface c |

Risk And Classification

Primary CVSS: v4.0 4.8 MEDIUM from security@pega.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/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: 0.000300000 probability, percentile 0.085830000 (date 2026-04-24)

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@pega.com | Secondary | 4.8 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N/E:X/C |
| 4.0 | CNA | CVSS | 4.8 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N |
| 3.1 | nvd@nist.gov | Primary | 4.8 | MEDIUM | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/L/I:L/A:N |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

None

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:N/SC:L/SI:L/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/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

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/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 | Pega | Pega Platform | All | All | All | All |

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-d26-vulnerability-remediat... | security@pega.com | support.pega.com | Vendor Advis |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, an |

Vendor Comments And Credit

Discovery Credit

CNA: Amjad Nayef Qabaha from Integrated Telecom Solutions (INOVAR) (en)

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