Pegasystems Security Bulletin for CVE-2017-17478

Pega has provided remediation for the following Common Vulnerabilities and Exposures (CVE): CVE-2017-17478.

CVE-2017-17478: Cross-Site Scripting

One cross-site scripting vulnerability is identified in this CVE. Versions 7.1.7, 7.1.8, 7.1.9, 7.1.10, 7.2, 7.2.1, and 7.2.2 of Pega Platform are affected.

In Designer Studio, a user with designer credentials can insert malicious code up to 64 characters into a text field, after establishing context. That XSS payload will execute when other Designer Studio users visit the affected pages.

Pega has determined a CVSS 3.0 score for this vulnerability:
CVSS 3.0 vector: AV:N/AC:L/PR:H/UI:R/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C
CVSS Base Score: 3.4
Impact Subscore: 1.4
Exploitability Subscore: 1.7
CVSS Temporal Score: 3.1
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 3.1

We would like to acknowledge Subin Varghese of Lakhshya Cyber Security Labs for reporting this vulnerability.

Remediation

Eliminating or blocking designer accounts on your deployed system can prevent this vulnerability. This is part of the security checklist for deploying applications provided by Pega.

If you have residual risk, a hotfix is available. To obtain the hotfix, submit a Support Request (SR) that includes your product version via the My Support Portal (MSP) to request the CVE Remediation fixes. Subsequently, you will be provided with the appropriate Pega Platform media.