



An arbitrary file-write vulnerability in Pega Browser Extension (PBE) affects Pega Robotic Automation version 22.1 or R25 users who are running automations that work with Google Chrome or Microsoft Edge.

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

Summary

CVE	CVE-2026-1078
State	PUBLISHED
Assigner	Pega
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 16:16:23 UTC
Updated	2026-04-08 21:27:00 UTC
Description	An arbitrary file-write vulnerability in Pega Browser Extension (PBE) affects Pega Robotic Automation version 22.1 or R25 u

Risk And Classification

Primary CVSS: v4.0 7.2 HIGH from security@pega.com

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

EPSS: 0.000410000 probability, percentile 0.125240000 (date 2026-04-09)

Problem Types: CWE-284 | CWE-284 CWE-284: Improper Access Control

Version	Source	Type	Score	Severity	Vector
4.0	security@pega.com	Secondary	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H/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:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

High

Sub Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pegasystems	Pega Robot Studio	affected 22.1	Not specified
CNA	Pegasystems	Pega Robot Studio	affected R25	Not specified

References

Reference	Source	Link	Tags
support.pega.com/support-doc/pega-security-advisory-a26-vulnerability-remediat...	security@pega.com	support.pega.com	
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: Ramon Dunker from Achmea, Security Assessment Team (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

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