



Cross-Site Request Forgery in PAC4J

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

Summary

CVE	CVE-2026-40458
State	PUBLISHED
Assigner	CERT-PL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 14:16:33 UTC
Updated	2026-04-20 14:41:43 UTC
Description	PAC4J is vulnerable to Cross-Site Request Forgery (CSRF). A malicious attacker can craft a specially designed website w

Risk And Classification

Primary CVSS: v4.0 7 HIGH from cvd@cert.pl

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

EPSS: 0.000190000 probability, percentile 0.049500000 (date 2026-04-20)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:L/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

High

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:L/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/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

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pac4j	Pac4j	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	PAC4J	PAC4J	affected 5.0 5.7.10 semver	Not specified
CNA	PAC4J	PAC4J	affected 6.0 6.4.1 semver	Not specified

References

Reference	Source	Link	Tags
www.pac4j.org/blog/security-advisory-pac4j-core-and-ldap.html	cvd@cert.pl	www.pac4j.org	Vendor Advisory
cert.pl/en/posts/2026/04/CVE-2026-40458	cvd@cert.pl	cert.pl	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Bartłomiej Dmitruk, striga.ai (en)

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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