LDAP Injection in PAC4J

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40459
State	PUBLISHED
Assigner	CERT-PL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-17 14:16:34 UTC
Updated	2026-04-20 14:38:27 UTC
Description	PAC4J is vulnerable to LDAP Injection in multiple methods. A low-privileged remote attacker can inject crafted LDAP syntax

Risk And Classification

Primary CVSS: v4.0 8.7 HIGH from cvd@cert.pl

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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: 0.002220000 probability, percentile 0.448230000 (date 2026-04-20)

Problem Types: CWE-90 | CWE-90 CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/C...
4.0	CNA	CVSS	8.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

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 4.0 4.5.10 semver	Not specified

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.