> Vulnerabilities in PAC4J software _

17 April 2026 | CERT Polska(../../../../author/cert-polska/) | #vulnerability(../../../../tag/vulnerability/), #warning(../../../../tag/warning/), #cve(../../../../tag/cve/)

CVE ID	CVE-2026-40458(https://www.cve.org/CVERecord?id=CVE-2026-40458)
Publication date	17 April 2026
Vendor	PAC4J
Product	PAC4J
Vulnerable versions	From 5.0 to 5.7.10 From 6.0 to 6.4.1
Vulnerability type (CWE)	Cross-Site Request Forgery (CSRF) (CWE-352(https://cwe.mitre.org/data/definitions/352.html))
Report source	Report to CERT Polska

CVE ID	CVE-2026-40459(https://www.cve.org/CVERecord?id=CVE-2026-40459)
Publication date	17 April 2026
Vendor	PAC4J
Product	PAC4J
Vulnerable versions	From 4.0 to 4.5.10 From 5.0 to 5.7.10 From 6.0 to 6.4.1

Vulnerability type (CWE)	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (CWE-90(https://cwe.mitre.org/data/definitions/90.html))
Report source	Report to CERT Polska

Description

CERT Polska has received a report about vulnerabilities in PAC4J software and participated in coordination of their disclosure.

The vulnerability CVE-2026-40458(https://www.cve.org/CVERecord?id=CVE-2026-40458): PAC4J is vulnerable to Cross-Site Request Forgery (CSRF). A malicious attacker can craft a specially designed website which, when visited by a user, will automatically submit a forged cross-site request with a token whose hash collides with the victim's legitimate CSRF token. Importantly, the attacker does not need to know the victim's CSRF token or its hash prior to the attack. Collisions in the deterministic String.hashCode() function can be computed directly, reducing the effective token security space to 32 bits. This bypasses CSRF protection, allowing profile updates, password changes, account linking, and any other state-changing operations to be performed without the victim's consent.

This issue was fixed in PAC4J versions 5.7.10 and 6.4.1

The vulnerability CVE-2026-40459(https://www.cve.org/CVERecord?id=CVE-2026-40459): PAC4J is vulnerable to LDAP Injection in multiple methods. A low-privileged remote attacker can inject crafted LDAP syntax into ID-based search parameters, potentially resulting in unauthorized LDAP queries and arbitrary directory operations.

This issue was fixed in PAC4J versions 4.5.10, 5.7.10 and 6.4.1

Credits

We thank Bartłomiej Dmitruk (striga.ai) for the responsible vulnerability report.

More about the coordinated vulnerability disclosure process at CERT Polska can be found at https://cert.pl/en/cvd/(https://cert.pl/en/cvd/).

(/en/)

computer security incidents. It carries out the role of CSIRT NASK, one of three such teams operating at the national level within the Polish national cybersecurity system.

ska_en)

LinkedIn(https://www.linkedin.com/showcase/cert-polska)

GitHub(https://github.com/CERT-Polska)

Incident reporting:
incydent.cert.pl(https://incydent.cert.pl/#!/lang=en)
cert@cert.pl(mailto:cert@cert.pl)

(../../../../../posts/2026/04/CVE-2026-40458/)

(/en/search)

Co-financed by the Connecting Europe Facility of the European Union