



An Lárionad Náisiúnta
Cibearshlándaála
National Cyber
Security Centre

NCSC #2607070212

NCSC Advisory

Critical Vulnerabilities in Joomla Content Editor (JCE) and SP Page Builder Extension CVE-2026-48907 and CVE-2026-48908

7th, July 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>. Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-48907**Published:** 2026-06-05**Vendor:** joomlacontenteditor.net**Product:** Joomla Content Editor (JCE) extension for Joomla**CVSS Score¹:** 10.0

Products Affected

Product	Version
Joomla Content Editor (JCE) extension for Joomla	1.0.0-2.9.99.4

Impact

A vulnerability in the JCE editor extension for Joomla allows the creation of new editor profiles for unauthenticated users, ultimately resulting in PHP code upload and execution.

Public proof-of-concept (PoC) exploits exist for this vulnerability, and mass exploitation has been observed.

Common Weakness Enumeration (CWE)²: CWE-284 Improper Access Control**Known Exploited Vulnerability (KEV) catalog³:** Yes**Used by Ransomware Operators:** N/A

¹ <https://www.first.org/cvss/>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Description

CVE ID: CVE-2026-48908**Published:** 2026-06-20**Vendor:** joomshaper.net**Product:** SP Page Builder extension for Joomla**CVSS Score⁴:** 10.0

Products Affected

Product	Version
SP Page Builder extension for Joomla	1.0.0-6.6.1

Impact

A vulnerability in SP Page Builder for Joomla allows unauthenticated users to upload arbitrary files, ultimately resulting in the upload and execution of PHP code.

Public proof-of-concept (PoC) exploits exist for this vulnerability, and mass exploitation has been observed.

Common Weakness Enumeration (CWE)⁵: CWE-434: Unrestricted Upload of File with Dangerous Type

Known Exploited Vulnerability (KEV) catalog⁶: No

Used by Ransomware Operators: N/A

⁴ <https://www.first.org/cvss/>

⁵ <https://cwe.mitre.org>

⁶ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from joomshaper.net and joomlacontenteditor.net.

CVE-2026-48907:

- <https://nvd.nist.gov/vuln/detail/CVE-2026-48907>
- <https://www.cve.org/CVERecord?id=CVE-2026-48907>
- <https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48907

CVE-2026-48908:

- <https://nvd.nist.gov/vuln/detail/CVE-2026-48908>
- <https://www.cve.org/CVERecord?id=CVE-2026-48908>
- <https://mysites.guru/blog/sp-page-builder-zero-day-uploadcustomicon-rce/>
- <https://www.joomshaper.com/forum/question/45152>