



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Friday, June 19, 2026

CAL-CSIC-202606-A-015

Joomla Content Editor Vulnerability

Joomla

KEV

Improper Access

JCE

The California Cybersecurity Integration Center (Cal-CSIC) has identified a maximum severity vulnerability in Joomla Content Editor (JCE). CVE-2026-48907, with a CVSS v4.0 score of 10, allows for improper access control to facilitate arbitrary code execution.¹ In addition, this vulnerability has been added to CISA's Known Exploited Vulnerability (KEV) catalog, and is currently under active exploitation.²³

When exploited, attackers can create new editor profiles for unauthenticated users, allowing for upload of malicious PHP: Hypertext Processor (PHP) code. Furthermore, Joomla stated that while patching closes the entry point, an already compromised site is still at risk.³

The Cal-CSIC recommends following Joomla's guidance on both mitigation and patching this vulnerability.

For more information on CVE-2026-48907, please refer to [JCE security update](#), [and a free patch for older sites](#)

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

References

¹ The Hacker News; "CISA Warns of Actively Exploited Joomla JCE Flaw Allowing PHP Code Execution"; <https://zeropath.com/blog/azure-bastion-cve-2025-49752>; accessed 19 June 2026

² CISA; "CISA Adds One Known Exploited Vulnerability to Catalog"; <https://www.cisa.gov/news-events/alerts/2026/06/16/cisa-adds-one-known-exploited-vulnerability-catalog>; accessed 19 June 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

³ Joomla Content Editor; "JCE Security Update, and a Free Patch for Older Sites";
<https://www.joomlacontenteditor.net/news/jce-security-update-and-a-free-patch-for-older-sites>; accessed 19 June 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR