CYBER ADVISORY

Tuesday, July 14, 2026 **CAL-CSIC-202607-A-007**

Maximum-severity Vulnerabilities Impacting Two Joomla Extensions

Arbitrary Code Upload	Full System Compromise	Remote Code Execution	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of two maximum-severity vulnerabilities relating to two separate Joomla extensions; both currently under active exploitation. CVE-2026-48939 is a Remote Code Execution (RCE) vulnerability contained in the iCagenda extension for Joomla. CVE-2026-56291 is an unauthenticated arbitrary upload vulnerability contained within the Balbooa forms extension for Joomla. Both CVEs carry a maximum-severity CVSS 3.1 score of 10.0.[1] [2]

CVE-2026-48939 is a vulnerability that enables an attacker to upload arbitrary files via the front-end file attachment feature without login, leading to PHP code upload and remote code execution. Successful exploitation allows the attacker to read all files, modify all data, and deny service – ultimately leading to full system compromise.[3]

CVE-2026-56291 is a vulnerability that permits attackers to upload executable files form any anonymous visitor with no login, no cross-site request forgery (CSRF) token, or check on the file type. Successful exploitation enables an attacker to upload a .php file into a public directory and run it to gain a foothold into the system and potentially pivot to other sites on the same hosting account.[4]

Both developers have acknowledged their respective vulnerability, and each have issued an update that will patch their respective CVEs. Prior to the new update, each vulnerability was actively being exploited as a zero-day as early as June 15, 2026. Please note that updating to the latest version merely closes the door on these vulnerabilities and does not fix an already compromised system. Both vulnerabilities have been listed on CISA's Known Exploited Vulnerabilities, and clients for both extensions are urged to update their extensions as soon as possible.

The Cal-CSIC recommends following each developer's update guidance as soon as possible. For additional details for each CVE, please use these links:

iCagenda Extension: https://mysites.guru/blog/icagenda-zero-day-file-upload-rce/#how-to-check-your-joomla-sites-for-icagenda-with-mysitesguru

Balbooa Extension: https://mysites.guru/blog/balbooa-forms-unauthenticated-file-upload-flaw/

Affected Product and Version

Product	Affected Version
iCagenda Extension for Joomla	3.2.1 – 4.0.7
Balbooa Forms Extension for Joomla	1.0 – 2.4.0

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] OpenCVE; "CVE-2026-48939"; https://app.opencve.io/cve/CVE-2026-48939; accessed 14 July 2026
[2] OpenCVE; "CVE-2026-56291"; https://app.opencve.io/cve/CVE-2026-56291; accessed 14 July 2026
[3] Mysites.guru; "Zero-Day Vulnerability Found in iCagenda Joomla Extension"; https://mysites.guru/blog/icagenda-zero-day-file-upload-rce/#how-to-check-your-joomla-sites-for-icagenda-with-mysitesguru; accessed 14 July 2026
[4] Mysites.guru; "Balbooa Forms Fixes an Unauthenticated File Upload RCE"; https://mysites.guru/blog/balbooa-forms-unauthenticated-file-upload-flaw/; accessed 14 July 2026