Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-56291: Balbooa Forms File Upload Flaw Actively Exploited

Date of Publication	Admiralty Code	TA Number
July 13, 2026	A1	TA2026196

Summary

First Seen: July 8, 2026
Affected Products: Balbooa Forms
Impact: CVE-2026-56291 is a critical (CVSS 10.0) unauthenticated arbitrary file upload flaw in the Balbooa Forms Joomla extension that allows any anonymous attacker to upload a malicious .php file and achieve full remote code execution in a single request. The vulnerability was exploited as a zero-day in the wild before a fix existed, and exploitation remains ongoing against unpatched sites. All versions up to and including 2.4.0 are affected; version 2.4.1 (released 9 July 2026) remediates the flaw. Organizations running Balbooa Forms should update to 2.4.1 immediately and inspect affected sites for signs of prior compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-56291	Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	Balbooa Forms	✓	✓	✓

Vulnerability Details

#1

CVE-2026-56291 is a critical unauthenticated arbitrary file upload vulnerability affecting Balbooa Forms, a drag-and-drop form-builder extension for Joomla (installed as the com_baforms component). The flaw is classed as CWE-434 (Unrestricted Upload of File with Dangerous Type) and carries a CVSS 4.0 base score of 10.0 (Critical), remotely exploitable in a single request, with no privileges or user interaction, culminating in full remote code execution.

#2

The root cause is a frontend attachment upload handler that performed no authentication, CSRF, or file-type validation. The endpoint accepted a file from any anonymous visitor with no login requirement and no allow-list on the file extension; while the filename was partially sanitized, that process did not reject a .php extension, so a caller-supplied .php file could be written into a public, PHP-executable directory and then invoked directly. Upload therefore converted straight into code execution, granting an attacker a server foothold with no account required on the target site.

#3

The vulnerability was exploited as a zero-day. It came to light through an abuse report on a live Joomla site, submitted as a raw web-server access log that evidenced active exploitation in the wild before any patch existed. Exploitation remains ongoing against unpatched instances.

#4

All versions up to and including 2.4.0 are affected; the flaw was remediated in version 2.4.1, released 9 July 2026, which hardens the upload path at four layers (server-side extension allow-list, MIME-type validation, forced server-side filenames, and a CSRF token check). Affected instances should be updated immediately and inspected for stray .php files in the upload directory and unrecognized Super User accounts, as pre-patch systems may already be compromised.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-56291	Balbooa Forms (`com_baforms`) for Joomla: all versions up to and including 2.4.0	cpe:2.3:a:balbooa:forms:*:*:*:*:*:joomla\!:*:*	CWE-434

Recommendations

Update the Extension Immediately: Upgrade every Balbooa Forms installation to version 2.4.1 or later without waiting for a scheduled maintenance window. This release closes the flaw at multiple layers and is the definitive fix; any site running 2.4.0 or earlier should be treated as actively exposed until it is updated. Because the changelog describes the fix in generic terms, do not defer the update on the assumption that it is routine housekeeping.

Inspect Upload Directories for Malicious Files: On any site that ran an affected version while exposed, examine the Balbooa Forms upload location at `images/baforms/uploads/` and its per-form subdirectories for any file that is not a legitimate image or document, and treat any `.php` or otherwise executable file there as a strong indicator of compromise. On a single host this can be checked over SSH by searching the upload path for PHP files, and any discovery should trigger incident response rather than simple deletion.

Audit Administrator Accounts: Review the Joomla user list, sorting by registration date, and treat any administrator or Super User account that no one recognizes or intentionally created as suspect. Code execution is a fast route to a hidden privileged account, so this check is essential on any site that was exposed, even after patching.

Restrict the Upload Endpoint Where Patching Is Delayed: If an installation cannot be updated immediately, unpublish any public form that accepts file attachments and, where feasible, block external access to the upload endpoint (`index.php?option=com_baforms&task=form.uploadAttachmentFile`) at the web application firewall or reverse proxy layer. As a defense-in-depth control, configure the server to prevent script execution within the `images/baforms/uploads/` directory.

Monitor and Hunt for Exploitation Activity: Review web server access logs for POST requests to the Balbooa Forms upload path originating from anonymous sources, and hunt for recently modified or unfamiliar PHP files across the site that may indicate planted persistence. Given confirmed in-the-wild exploitation prior to the patch, prioritize retrospective log review on any historically exposed asset.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1136: Create Account	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Impact	T1491: Defacement	

Patch Links

https://www.balbooa.com/help/joomla-forms-documentation/basics/changelog

https://www.balbooa.com/joomla-forms

References

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

https://www.cycognito.com/blog/emerging-threat-cve-2026-56291-balbooa-forms-remote-code-execution-via-unauthenticated-file-upload/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 13, 2026 • 07:30 AM

More at www.hivepro.com