cnMaestro is not affected by PHP2Shell

CVE-2026-109618 and CVE-2026-109619

> **Status: not affected.** No action is required for cnMaestro customers.

PHP2Shell is the name given to two critical vulnerabilities in the PHP engine, disclosed and patched by the PHP project on 21 October 2026.

CVE	Issue
CVE-2026-109618 GHSA-w8hw-w9fx-j79w	Memory corruption when PHP runs out of memory while parsing a multipart request body.
CVE-2026-109619 GHSA-6wmf-4rv5-p3rp	Stale global state carried between requests on the same worker, leading to use-after-free and memory disclosure.

Both are rated **CVSS v4.0 9.2 (Critical)**. They are exploitable remotely over HTTP without authentication and can result in remote code execution as the web worker account, or disclosure of memory from other requests, including credentials and tokens. Exploitation in the wild has been reported.

Affected: any PHP installation serving web requests (PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, LiteSpeed) earlier than PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35.

Why cnMaestro is not affected

The vulnerabilities exist only in the PHP interpreter and runtime. cnMaestro does not include, bundle or depend on any PHP components, so the vulnerable code is not present and there is no attack surface for these CVEs.

The same applies to CVE-2026-115560, a separate, lower-likelihood PHP issue announced by the PHP Foundation after the PHP2Shell disclosure.

Recommended actions

cnMaestro	None required.
Other systems	If you run PHP-based web applications elsewhere (for example WordPress, Drupal, Joomla or custom PHP apps), patch PHP to a fixed release as a priority. WAF rules reduce exposure but do not replace patching.

We will update this notice if our assessment changes.