PHP 漏洞暫時緩解機制

協助企業在正式更新前降低特定攻擊路徑風險

適用議題　CVE-2026-109618 與 CVE-2026-109619

相關 PHP 漏洞可能導致未經授權的遠端程式碼執行。我們提供設定緩解腳本，協助企業在相容性驗證或維護排程期間先降低風險，並銜接後續正式更新。

客戶可以獲得什麼

- 檢查支援範圍內的 PHP 版本、啟用狀態及相關緩解設定。
- 以管理員層級套用指定設定，降低一般應用設定覆寫的機會。
- 提供變更前備份、設定語法檢查、服務重新載入與執行結果輸出。
- 可設定試跑模式，先評估預計變更，再依維護流程安排部署。

提供的緩解方式

對應漏洞	緩解方向	客戶需了解的影響
CVE-2026-109618	調整 PHP 記憶體限制，減少可預測的記憶體不足觸發條件。	取消 PHP 自身的記憶體用量上限，需評估資源耗盡風險。
CVE-2026-109619	停用 session 上傳進度；PHP 8.5 另停用致命錯誤的自動堆疊追蹤。	依賴相關進度功能的流程及部分錯誤診斷資訊可能受影響。

適用環境

主要自動套用對象為 Linux 上的 PHP-FPM 與 Apache mod_php。實際可用性須依 PHP 版本、套件來源、設定檔位置與服務架構確認。

建議部署流程

確認環境 → 評估影響 → 試跑與備份 → 套用與驗證 → 正式更新。

這是設定層的暫時緩解，並未更新 PHP 套件或修補其程式碼；緩解後仍有殘餘風險，應持續完成正式安全更新。

歡迎與我們聯繫，確認您的環境是否適合採用。

部署前應了解的事項

設定調整與功能影響

CVE-2026-109618　PHP 記憶體限制

將 memory_limit 設為 -1，取消 PHP 記憶體限額。請求或高併發可能耗盡資源，需評估 RAM、swap 與監控；腳本不會自動建立外部記憶體限額。

CVE-2026-109619　上傳進度與錯誤診斷

session.upload_progress.enabled=0；PHP 8.5 另設 fatal_error_backtraces=0。一般上傳與整個 session 未被停用；依賴進度資料的流程可能失效，致命錯誤診斷資訊可能減少。

會影響哪些服務與套件

修改 FPM pool 或新增 Apache PHP 設定後會重新載入服務。同一實例的其他 pool 及網站可能受影響，需安排測試與維護時段。

類型	處理範圍
PHP-FPM 與 Apache PHP 模組	調整其 Web PHP 執行設定，不替換執行檔或變更套件版本。
CGI、LiteSpeed LSAPI、FrankenPHP	本腳本沒有自動套用流程；需另行評估處理方式。
CLI、Windows IIS、自訂或容器環境	CLI 不是本次修改對象；其餘環境需另確認適用性與部署方式。

部署與還原的重要限制

固定路徑偵測可能漏掉自訂設定或多實例。設定檢查與結果輸出仍須以實際 Web 值、worker 更新及應用驗證確認。

失敗時可能已有部分設定變更。還原檔案後仍須重新載入與驗證；完整備份可能覆蓋後續修改，部署不保證零中斷。

本機制無法取代正式修補，亦不保證阻擋所有利用路徑。實際適用與部署安排以環境評估為準。

參考來源　PHP 官方安全公告

CVE-2026-109618　https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w

CVE-2026-109619　https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp