關於 PHP2Shell 與 HTTP2Shell 漏洞之影響評估聲明

發布日期：2026 年 10 月 30 日

近期公開揭露 PHP2Shell（CVE-2026-109618、CVE-2026-109619）及 HTTP2Shell（CVE-2026-111497）重大資安漏洞。竣盟科技已第一時間針對旗下 LogMaster 產品進行安全檢視與影響評估。經確認，目前上述漏洞均未對 LogMaster 造成直接影響，說明如下：

一、漏洞影響評估

1. PHP2Shell（CVE-2026-109618、CVE-2026-109619）：LogMaster 未使用 PHP 執行環境或相關元件，因此不受本次漏洞影響。

2. HTTP2Shell（CVE-2026-111497）：LogMaster 部分內部元件涉及本次漏洞相關技術，但均部署於 Docker 容器隔離環境，未直接對外提供服務。經評估，目前未發現外部攻擊者可直接利用此漏洞影響 LogMaster 的攻擊途徑。

二、後續安全強化措施

爲持續提升產品安全性，竣盟科技預計於 LogMaster 5.1.1.6 版本更新相關元件，並持續追蹤漏洞研究進展及原廠安全公告，定期檢視產品元件與部署環境的安全性。如有需要客戶配合處理的事項，將另行通知。

三、客戶與合作夥伴建議

若貴單位另有獨立部署 PHP、Node.js、Brotli 或其他可能受影響的系統與服務，建議依各原廠安全公告進行檢查，並儘速完成必要的安全更新。

竣盟科技將持續落實產品漏洞管理與安全維護，確保 LogMaster 的穩定運作及資訊安全，敬請客戶與合作夥伴安心使用。

竣盟科技股份有限公司

2026 年 10 月 30 日

參考資料：美國國家漏洞資料庫（NVD）官方漏洞紀錄，請參閱上述 CVE 連結。