

TrendLife PHP 漏洞急救包

別讓 PHP 漏洞危害您的網站安全

提供 7 天免費服務

方案總覽 (Solution Overview)

2026 年 10 月 21 日，PHP 團隊公布了兩項重大漏洞：CVE-2026-109618 與 CVE-2026-109619 (統稱 PHP2Shell)，並釋出修補版本。

即使網站伺服器只有一個未修補的 PHP 漏洞，也可能導致服務中斷、資料外洩或遭到未授權存取。這兩項漏洞允許攻擊者在未登入的情況下，在伺服器上遠端執行惡意程式碼。每項漏洞的評分皆高達 9.2 (CVSS v4.0)，且在官方修補程式正式發布前，攻擊利用程式碼 (Exploit) 就已被公開。

如果您自行架設或管理網站，請先確認目前使用的 PHP 版本，並安裝最新的安全性更新。

如果網站仍使用 PHP 8.1 或更早版本，建議向主機服務商確認是否已完成漏洞修補，因為部分服務商或 Linux 發行版本仍可能提供安全性修正，不能只憑版本號判斷網站是否安全。

調整伺服器設定雖然能暫時降低部分風險，但仍無法取代正式的安全性更新。

抵禦 PHP2Shell 攻擊



抵禦 PHP2Shell 攻擊 (Protection Against PHP2Shell Attacks)

TrendLife PHP 漏洞急救包 為您的網站增加一層防護，在 PHP2Shell 及其他網路攻擊抵達伺服器之前，協助攔截威脅。在您完成官方安全性更新之前，這項服務可提供暫時性的防護，但無法取代正式的漏洞修補。

TrendLife PHP 漏洞急救包 可協助防範 PHP2Shell 及其他已知的 PHP 攻擊，並針對 PHP、WordPress 和 Laravel 網站最佳化安全防護規則。服務設定簡單、內含免費 SSL 憑證，讓您在修補漏洞期間，降低網站遭受攻擊及服務中斷的風險。

為協助網站經營者因應此次資安威脅，TrendLife 提供 **7 天免費防護服務**，自服務啟用防護當天開始計算。免費期結束後，您可以選擇訂閱 TrendLife PHP 漏洞急救包，持續保護網站安全。

TrendLife PHP 漏洞急救包 主要功能與效益 (Key Features and Benefits)

- **雲端服務：服務可於 AWS 雲端平台上運行**，提供網站安全防護服務。

- **支援多個網站：**可為企業旗下的不同網站，分別建立及管理防護服務。
- **設定簡單：**約 20 至 30 分鐘即可完成設定，並支援使用 Google 帳號登入 (Google OAuth) 。
- **7 天免費防護：**正式訂閱前，可免費使用 7 天防護服務。
- **訂閱與購買：**免費期結束後，可購買或續訂 TrendLife PHP 漏洞急救包，也可透過 Worry-Free 相關方案取得服務。詳情請洽當地服務合作夥伴，例如託管服務供應商 (MSP) 。
- **單一帳號管理多項服務：**一個帳號即可設定及管理多項防護服務。每項服務最多可保護同一主網域下的 10 個主機名稱 (Hostnames) 。
- **支援 MSP 集中管理：**託管服務供應商 (MSP) 可透過專用的管理帳號，集中管理更多防護服務。

設定指南：網站防護 (約 20 至 30 分鐘)

1. 前往 TrendLife PHP 漏洞急救包

前往 <https://waf.trendlife.com>，點選「Get started (開始使用)」。

2. 新增您的網站

為您的防護服務命名，並輸入訪客用來造訪網站的網域名稱 (例如 www.customer.com) 。

每項服務可保護同一主網域下的最多 10 個主機名稱。

3. 輸入主機託管資訊

輸入您網站目前託管的伺服器主機名稱 (例如 origin.example.com) 或公開 IP 位址 (Public IP) 。

4. 選擇憑證

請選擇下列其中一種方式。憑證必須涵蓋與此服務關聯的所有主機名稱，我們會在設定時進行驗證。

- **自動核發憑證：**TrendLife 會免費自動核發及更新 SSL 憑證。您只需新增一筆 DNS 紀錄，完成網域所有權驗證。
- **使用現有憑證：**您也可以自行上傳既有的 SSL 憑證，但必須在憑證到期前自行更新及替換。

5. 檢查您的設定

在啟用防護前請仔細檢查各項設定。服務建立後即無法修改這些設定；若需更改，必須刪除該服務並重新建立。

6. 啟用防護

點選「Activate Protection (啟用防護)」開始保護。

您的 **7 天免費服務** 將從啟用防護後開始計算。

7. 設定原始伺服器防火牆 (必要步驟)

請與您的網路管理員聯絡，將 TrendLife 提供的 CDN/WAF IP 位址範圍加入原始伺服器防火牆的允許清單 (Allowlist)。

這項設定可讓來自 TrendLife CDN/WAF 的 HTTPS 流量順利連線至您的網站伺服器。

8. 測試網站連線

透過 TrendLife CDN/WAF 測試網站，確認以下項目皆正常運作：

- TLS 安全連線設定
- 網站流量轉送至原始伺服器的路徑
- 網站各項功能

請注意： 在此步驟期間，直接存取原始伺服器的管道仍會保持開啟。

9. 更新 DNS 設定 (必要步驟)

請與您的網路管理員合作，將網站的 DNS 紀錄指向 TrendLife CDN 節點。

完成後，請確認網站流量已透過 TrendLife CDN/WAF 傳送，讓防護機制生效。

10. 鎖定原始伺服器防火牆 (必要操作)

在 DNS 切換與驗證完成後，請配合您的網路管理員，調整原始伺服器的防火牆設定。

移除允許其他來源直接存取原始 Web 服務的防火牆規則。僅保留 TrendLife 提供的 CDN/WAF 來源 IP 範圍，以及必要的管理與維運存取規則。

聯絡與支援 (Contact & Support)

- 聯絡 TrendLife : Trendlife_Contact@trendmicro.com
- 更多資訊 : <https://trendlife.com/zh-tw>