

後端程式語言安全缺陷 黑客可掌控服務器

PHP 爆漏洞 危及全球七成網站

全球約 70% 網站採用的後端程式語言 PHP，於 10 月 21 日爆出被安全人員稱為「PHP2Shell」的兩項重大安全漏洞，編號分別為 CVE-2026-109618 和 CVE-2026-109619。這些漏洞一旦被成功利用，黑客便能在未經授權情況下掌控服務器，對企業與個人網站構成極大信息安全威脅。漏洞被揭露後，網站營運者急忙採取保護措施，歐洲等地的政府網站一度大量離線。PHP 開發團隊表示，已上線修復該兩處嚴重漏洞的更新，並強烈建議用戶立即更新。



■後端程式語言 PHP 存在漏洞，黑客可在未經授權情況下掌控服務器。 網上圖片

PHP 是一種廣泛用於服務器端的開源編程語言，用戶登錄網站、搜索商品、提交評論時，服務器都需處理請求、訪問數據庫並返回相應內容，PHP 便承擔其中部分工作。WordPress 等內容管理系統，以及大量電商平台、論壇、媒體網站和企業應用，都可能依賴 PHP 運行，故用戶未必了解 PHP，但每天都在使用由其提供支持的服務。

今次發現的漏洞，在 CVSS v4.0 漏洞嚴重性評級中被評為 9.2 級（上限 10 級），屬嚴重級別。歐盟電腦緊急應變小組日前在諮詢報告中指出，9.2 級表明存在未經身份驗證的遠端程式碼執行風險，即允許攻擊者在不登入的情況下，在受攻擊系統上運行惡意程式碼。PHP 官方披露，其中一項漏洞涉及內存不足時的異常處理，程式內部數據尚未完成初始化，後

續清理過程卻可能將其當作正常數據處理；另一項漏洞則可能導致服務器錯誤使用已釋放的失效內存，使攻擊者有機會讀取敏感數據。

藉 OpenAI 模型發現缺陷

《華爾街日報》報道，美國安全公司 Calif 今年較早時藉着 OpenAI 旗下人工智能（AI）模型 GPT-5.6 Sol，發現該關鍵缺陷，並通報 PHP 官方。安全公司 Wiz 也獨立發現兩項漏洞。

漏洞確認後，PHP 維護者與研究機構、雲服務商和安全公司花費數周進行修復，共涉及近 200 萬個文檔、逾 1 萬行代碼。安全更新原定於 22 日發布，但因兩個漏洞的 CVE 編號 20 日便已在網絡流傳，PHP 團隊隨即提前公布安全預告，並將正式發布時間提前一天。豈料預告發

布後半小時，Calif 意外公布一段概念驗證（PoC）視頻，透露部分漏洞技術細節。21 日，PHP 按提前後計劃，發布 PHP 8.5.12、8.4.27、8.3.36 和 8.2.35 四個安全補丁，覆蓋仍受支持的版本分支。

據 PHP 基金會發布的事件覆盤，其中一類內存管理風險早在 2024 年就被發現，但當時核心開發人員未找到潛在的具體攻擊路徑。而由於修復方案可能影響舊程式兼容性、性能及第三方擴展，維護團隊未能及時就解決方案達成一致，修復工作因此數次停滯。

為防範潛在風險，包括法國、德國、荷蘭和比利時在內的歐洲多國政府網站，已暫時關閉部分服務；美國網絡論壇 Something Awful 和維基百科部分服務也已下線；日本部分託兒中心系統和線上遊戲服務同樣採取預防性措施。

法騷亂嚇退遊客 「災難性」衝擊旅業

法國多地爆發暴力騷亂，警民衝突、建築物起火及商店遭搶掠的畫面傳遍全球，令外國遊客對赴法旅遊的安全產生疑慮。旅遊業界指出，巴黎等主要城市的酒店預訂已出現放緩迹象，若騷亂持續數周甚至數月，恐對法國旅遊業造成嚴重衝擊。法國旅遊機構聯合組織負責人卡薩涅表示，尼斯、巴黎及里昂市中心的暴力事件對旅遊業造成「災難性」影響。

旅遊諮詢公司 Protourisme 負責人阿里諾亦指出，巴黎、里昂及馬賽等主要城市的酒店預訂已經轉弱。他估計，巴黎市中心每發生一日騷亂，可能導致隨後數日及數周的酒店取消率達到約 1%。他以 2026 年預計 4,200 萬個酒店住宿夜次計算，認為這次騷亂的衝擊不算大，但不能低估暴力事件反覆發生的累積影響。

法國每年接待約 1 億人次遊客，旅遊消費超過 700 億歐元（約六千一百六十七億港元），旅遊業因此高度關注騷亂對國際形象的影響。

業界估計至少 3000 店鋪受損

另外，近日示威引發的嚴重暴力衝突與搶掠事件，導致全國至少 3,000 家店鋪受損。保險業界預計，是次騷亂將造成高達 12 億歐元（約 106 億港元）的巨額損失。



■巴黎抗議活動後，遊客走過遭洗劫破壞的商店。 美聯社

胡塞武裝沙特續互襲 美縮減中東駐軍

近期也門胡塞武裝和沙特阿拉伯持續互襲，美國駐沙特大使館於 21 日發布安全警報，稱敵對行動可能迅速升級並蔓延至周邊地區。美國全國廣播公司（NBC）同日引述兩名知情人士報道，美軍近期一直在悄悄縮減其在中東各基地的駐軍規模，美國務院也已下令進一步削減駐該地區多個外交機構的人員。

報道稱，一名美國官員和兩名知情人士透露，美軍駐約旦基地的人員已被調離，美軍駐卡塔爾和科威特基地的人員也



■在也門傑巴爾漢前線，也門政府軍發炮與胡塞武裝交戰。 法新社

在撤離範圍內。此次撤離消息爆出，正值美軍官員向總統特朗普提交重新打擊伊朗方案。多名消息人士指出，此次撤離與 2 月美伊衝突爆發後啟動的軍事基地和使館撤離計劃類似。

美以傳已擬定中選後再襲伊

另外，《紐約時報》引述美國官員及知情人士報道，國防部長赫格塞思日前訪問以色列時，與以總理內塔尼亞胡討論新一輪針對伊朗的攻擊，美以軍方已擬定具體計劃，準備於美國中期選舉過後，重新對伊發起空襲。

伊朗官員則警告，若戰火重燃，報復範圍將可能擴展至中東地區的數據中心和海底網絡線纜。伊朗伊斯蘭革命衛隊發言人穆赫比 21 日則表示，正準備推出一款他稱為「炸彈之父」的新武器，「我們將向敵人展示新東西，有史以來威力最大的炸彈。美國此前曾使用『炸彈之母』，現在我們準備推出『炸彈之父』。」

美食品商控特朗普越權向加國徵稅

美國新澤西州食品進口商蓋勒特集團（Gellert Global Group）入稟美國國際貿易法院，控告總統特朗普今年 7 月引用上世紀三十年代大蕭條時代的《斯姆特-霍利關稅法》第 338 條，對包括乳製品在內的加拿大產品徵收 50% 關稅，超越了總統的權力，違反憲法。蓋勒特指稱特朗普引用這條生效 96 年但從未被實際援引的法規，導致集團每年增加 4,000 萬美元（約 3.12 億港元）財務負擔。

指近百年法規波及供應鏈

這宗訴訟由非牟利的維護公共利益法律事務所 Liberty Justice Center，代表蓋勒特集團提出控告。Liberty Justice Center 一直不停應對特朗普的關稅政策，負責人阿爾布雷希特指出，任何總統都不應擁有

隨意啟用一條塵封已久法規的權力，並在不受國會限制下，以此法規徵收大範圍的關稅或禁止進口。

蓋勒特集團聯席行政總裁蓋勒特表示，該集團多年來一直致力與食品業的供應商、客戶和合作夥伴建立互信關係，但特朗普引用近 100 年前的關稅法規，導致這些良好關係在一夜之間擾亂，並造成成本大增和不确定性，影響波及整條供應鏈。他指出蓋勒特集團正遭受貿易戰四面夾擊，既要為進口的加拿大乳酪支付 50% 關稅，也需面對加拿大政府徵收報復性關稅，說明關稅爭端如何擾亂北美的一體化市場。

■特朗普向加拿大徵收關稅，再次受到美國企業入稟法院挑戰。 路透社

