

香港文匯報訊 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。

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。

OpenAI 模型發現關鍵缺陷

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，即允許攻擊者在未登入的情況下，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。

《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，Google隨後也披露旗下AI模型Gemini 4 Argon曾參與漏洞發現、開發及檢測安全補丁的驗證工作。

PHP急修復 多地機構網站離線

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。儘管視頻隨後被刪除，但副本仍在社媒流傳，推動其他PoC加速開發並進一步擴散。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基金會發布的事件復盤，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。PHP基金會坦承，其核心開發團隊共13人，分布在8個國家，多數開發者為兼職，因團隊規模有限，且承擔多項維護任務，安全決策機制和資源不足共同導致此次修復延誤。

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，已預防性暫時關閉部分服務；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。新加坡網絡安全局警告，PHP所有版本均受影響，當地網絡安全公司WatchTower監測發現，其誘捕服務器網絡已記錄到針對這兩項漏洞的攻擊嘗試。澳洲網絡安全中心則已發布最高級別的關鍵警報，敦促所有組織清查環境中所有PHP的執行實例。



● PHP是一種廣泛用於服務器端的開源編程語言。圖為西班牙程式員使用PHP。

路透社

中美官方機構：更新是唯一安全解決方案

香港文匯報訊 面對「PHP2Shell」這一CVSS評分高達9.2的嚴重漏洞，包括中國工業和信息化部網絡安全威脅和漏洞信息共享平台（NVDB）和美國國家安全局（NSA）在內的官方機構表示，立即更新是唯一徹底的安全解決方案，在無法立刻更新的情況下，則需採取連串臨時緩解措施來降低風險。

NVDB通報，PHP是一種廣泛用於網站開發的開源服務器端腳本語言，此次發現的兩項遠

程代碼執行漏洞危害嚴重，黑客可在未經身份驗證情況下遠程執行任意代碼，造成服務器被控制、敏感信息洩露及業務中斷等嚴重後果，建議相關機構和用戶立即展開全面排查，並及時升級至最新安全版本，以防範網絡攻擊。

PHP在官方發布的安全建議中，明確表示「沒有任何完整的緩解措施，更新是唯一安全的選擇」。

NSA等機構則建議，若無法立刻更新，可採

取部分臨時措施降低風險，如系統下線、啟用Web應用防火牆、遵循PHP官方提供的降低特定攻擊路徑暴露面的建議等，但它們不能替代更新，系統仍不安全。

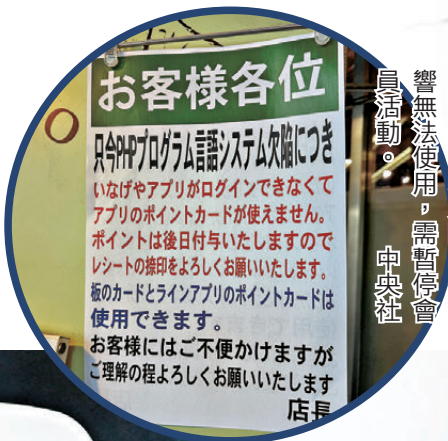
此外，PHP維護團隊21日發布的安全更新中，僅包含目前仍受支持的較新版本，針對PHP8.1及以前版本的支持已停止，NSA據此建議替換8.1及以下版本的PHP服務，因它們無法獲得補丁。

熱門後端程式語言 黑客可在未經授權下掌控服務器

PHP爆嚴重安全漏洞 全球七成網站受威脅



●英國國家網絡安全中心呼籲英國機構即時作出保護行動。路透社



●日本超市告示指，由於應用程式受駭事件影響無法使用，需暫停會員活動。中央社



港數字辦高度關注 要求各部門機構盡快更新

香港文匯報訊 香港數字政策辦公室（DPO）22日表示，高度關注全球網站廣泛應用的後端程式語言PHP的嚴重安全漏洞，數字政策辦公室已要求所有政府決策局/部門及公營機構，即時全面檢視其資訊系統有否受影響，並須盡快更新安全補丁，否則相關系統須暫時離線或隔離，以降低被入侵風險。同時，DPO已為所有政府決策局/部門主頁的寄存或託管的網站更新安全補丁，且目前未接獲有關網絡保安事故報告。

議員籲加強支援中小企資安技術

立法會議員吳傑莊對事件高度關注與憂慮，指出PHP支撐全球約七成網站的後端系統，目前全球多國政府網站已受波及，更有大型網絡服務器預防性停機，這是一場不容忽視的全球性資安危機。

他表示，香港需以最高規格因應外流的攻擊程式碼攻擊。他建議政府加強對中小企資安技術的支援力度，並聯合本地科技業界及商會，向中小企發出廣泛的簡易升級指南與安全預警，因這類企業普遍缺乏專職資安人員，是黑客最容易突破的缺口。長遠來看，政府還應建立「網絡安全主動防護」與「企業數據洩露賠償」機制，加速推動網絡安全立法，並擬定企業數據洩露賠償與懲罰機制，倒逼企業和機構提高對科技基建更新與維護的重視。同時，香港應牽頭與粵港澳大灣區其他城市建立「開源軟件安全漏洞聯合通報與AI輔助檢測機制」，利用大灣區的AI算力優勢，主動預判並應對未來更複雜的跨境網絡威脅。

美警告胡塞戰火蔓延周邊 撤駐沙特非緊急僱員及家屬

香港文匯報訊 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。

縮減中東基地駐軍規模

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，這些舉措是因該地區美國設施存在被伊朗及其盟友胡塞武裝打擊的風險。

路透社引述多名美國官員稱，美國務院已下令部分外交官及其家屬撤離沙特，並計劃撤離中東其他一些國家的外交官和家屬。不過美國務院發言人皮戈特隨後在社媒發文稱，相關說法不準確，國務院僅向駐沙特的「非緊急」政府僱員及家屬下達撤離命令，「國務院官員及家屬的安全是最優先事項，我們將繼續採取一切措施保護他們。」



●胡塞武裝與也門政府軍交火地區冒起濃煙。法新社

美防長訪以目的 傳擬定中選後重新攻伊

香港文匯報訊 《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。

報道稱，美以正規劃一場時間短、強度高的軍事行動，已有以空軍軍機飛過伊拉克上空進行演練，潛在打擊目標包括伊朗能源基礎設施、核設施，以及導彈與無人機武器庫。部分美官員認為，再發動一次大規模攻擊，可能把伊朗經濟推到崩潰邊緣，迫使伊方在歷時8個月的軍事衝突後，作出外交讓步。

然而美國總統特朗普會否批准此次攻擊方案仍未確定，因他今年已多次否決重啟大規模戰鬥的方案。外界亦懷疑新一輪戰爭能否較今年2月開戰初期美以聯軍對伊朗狂轟濫炸，取得更好戰果。當時密集的攻擊推高全球能源價格與通脹，並大幅消耗美軍防空攔截彈庫存。

伊警告推出「炸彈之父」

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』。」



●赫格塞思早前秘密訪問以色列。彭博社

美企控特朗普引用陳年法規徵關稅違憲

香港文匯報訊（特約記者 劉正言）美國新澤西州食品進口商蓋勒特集團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。

當加拿大和美國之間的貿易談判破裂後，特朗普援引鮮為人知的大蕭條時期《關稅法》，對乳製品、酒類、傢具，甚至曲棍球棒在內的加拿大進口商品徵收50%懲罰性關稅。

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的法規的權力，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。這是特朗普因關稅政策權限面對的最新法律挑戰，蓋勒特集團的訴訟要求法院宣布這些關稅非法，並下令退還關稅及利息。

擾亂北美一體化市場

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確定性，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，說明關稅爭端擾亂北美的一體化市場。

加拿大奶酪供應商從美國紐約州北部的農場採購牛奶，這些牛奶在加拿大加工成為奶酪，然後再運回美國出售。