

AI助揭PHP安全漏洞 多國政府網站急下線

中國工信部發風險提示 建議升級至最新版本

多國網絡安全機構21日發布警告指，網安公司使用人工智能（AI）工具，發現廣泛用於網站開發的PHP腳本語言存在兩個嚴重安全漏洞，黑客可能利用這些漏洞奪取服務器控制權。PHP開發團隊當天發布緊急安全更新修復漏洞，但黑客近日已嘗試發動數百萬次攻擊，大量網站臨時關閉以降低風險，包括法國、英國、日本等國的官方機構網站。中國工業和信息化部（工信部）22日發布風險提示，建議相關單位和用戶及時升級至最新安全版本，或採取臨時防護措施。

【大公報訊】PHP基金會21日發布緊急安全更新，修復兩個嚴重安全漏洞。據報道，這些漏洞已存在十多年，未經身份驗證的攻擊者可能利用相關漏洞遠程執行代碼，奪取服務器控制權，造成敏感信息洩露、業務中斷等後果。總部位於美國加州的網絡安全公司Calif於今年8月使用OpenAI公司的GPT-5.6 Sol模型發現相關漏洞。同一時間，谷歌母公司Alphabet旗下網安公司Wiz也報告稱，其研究團隊使用自研工具和谷歌Gemini 4Argon模型發現了這些漏洞。

或影響全球約3000萬個網站

PHP是一種廣泛使用的服務器端腳本語言。它在服務器上運行，用於生成網頁內容、與數據庫交互，也被大量集成到其他產品中。在能辨識服務器端腳本語言的網站中，約70%至75%使用PHP。英國薩里大學網絡安全中心教授伍德沃德警告說，新發現的安全漏洞可能影響全球大約3000萬個網站。網絡基礎設施公司Cloudflare行政總裁普林斯22日稱，近日已檢測到數百萬次試圖利用這些漏洞的攻擊行為。目前尚無相關網絡攻擊造成實際損失的報告。

中國工信部網絡安全威脅和漏洞信息共享平台（NVDB）22日發布風險提示，指出PHP存在兩個遠程代碼執行超危漏洞，危害嚴重。NVDB建議相關單位和用戶立即開展全面排查，及時升級至最新安全版本，或採取臨時下線、關閉會話上傳進度功能、網絡隔離、網絡訪問限制等臨時防護措施；加強網絡安全監測和管理，及時修改賬號、口令和密鑰等憑證，防範網絡攻擊風險。

美國白宮21日發表聲明稱，正與各聯邦機構及主要AI企業合作，保護美國的網絡和重要基礎設施。英國國家網絡安全中心敦促相關機構立即升級系統，若無法及時修復，應考慮暫時關閉受影響網站。澳洲信號局發布警告，敦促企業及用戶盡快完成更新。法國、英國、芬蘭、荷蘭等多個歐洲國家的部分官方機構網站21日紛紛關閉，德國和奧地利等國的部分大學網站也暫時下線。

日本政府22日呼籲各網站運營方採取措施，日本中央和地方政府部門、鐵路、金融機構的多個網站暫停訪問或暫停部分網站服務，首相高市早苗22日一度關閉個人網站，全日空等多家日本企業亦暫停部分網站服務。

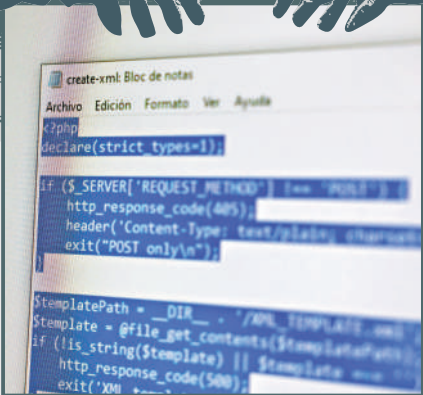
專家：普通用戶無需恐慌

PHP基金會近期在保密狀態下進行修復工作，原計劃22日正式公開相關信息並同步發布安全更新。然而，關於兩個漏洞的消息於20日在社交媒體上洩露，一些黑客隨即嘗試發動攻擊，PHP基金會不得不將發布更新的時間提前至21日。澳洲莫納什大學教授霍達警告說，在這種混亂情況下，網絡詐騙風險也將提升。不法分子可能利用重大網絡安全事件製造恐慌，誘導用戶點擊虛假的「安全更新鏈接」或提供個人信息。

網安專家表示，普通用戶無需恐慌，因為PHP運行在服務器上，而非個人上網設備裏。如果某個網站暫時打不開，可能是主動避險行為。若網站後續發布了數據洩露通知，用戶可根據提示採取更換密碼等安全措施。（綜合報道）



▲全日空22日宣布，受PHP安全漏洞影響，該公司網站的部分功能暫時無法使用。圖為全日空在羽田機場的櫃檯。 法新社



▲PHP是一種廣泛使用的服務器端腳本語言。 路透社

PHP安全漏洞Q&A

PHP是什麼？

PHP是一種廣泛使用的服務器端腳本語言。它在服務器上運行，用於生成網頁內容、與數據庫交互，也被大量集成到其他產品中。在能辨識服務器端腳本語言的網站中，約70%至75%使用PHP。

發現了什麼漏洞？

今年8月，網絡安全公司Calif使用OpenAI旗下的人工智能（AI）模型GPT-5.6 Sol，找到兩個潛藏在PHP代碼庫中的高危漏洞。同一時間，谷歌母公司Alphabet旗下的網絡安全公司Wiz也報告稱，使用自研工具和谷歌Gemini 4Argon模型發現了這些漏洞。

這兩個漏洞已存在十多年。攻擊者可能通過觸發內存耗盡狀態，造成內存損壞，並在特定條件下利用漏洞遠程執行代碼，從而奪取服務器控制權。

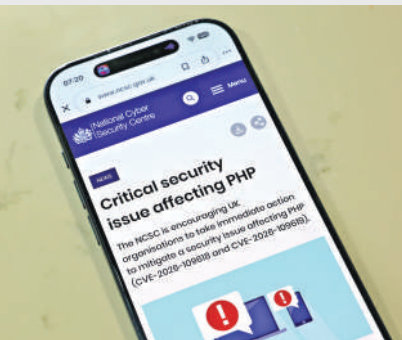
哪些網站受影響？

PHP開發團隊21日發布緊急更新，修復上述漏洞。但由於一些黑客已嘗試發動網絡攻擊，很多網站臨時關閉以降低安全風險。

德國、法國、英國、比利時、芬蘭、荷蘭等國的部分官方機構網站21日紛紛關閉。日本首相高市早苗等官員22日一度關閉個人網站，厚生勞動省亦關閉護理服務信息公開系統的網站。

美國網絡論壇Something Awful和維基媒體基金會旗下的維基百科部分支援服務也臨時下線。

大公報整理



▲英國國家網絡安全中心發布關於PHP安全漏洞的警報。 路透社

黑客亦可用 AI工具成「雙刃劍」

【大公報訊】據路透社報道：網絡安全研究人員近期在人工智能（AI）工具的幫助下，發現PHP存在潛藏多年的重大漏洞。美國雲網絡安全服務公司首席技術官克內克特表示，AI模型將不斷在廣泛使用的軟件中發現類似漏洞，軟件維護者、研究人員和政府



▲美國民眾5日在紐約示威，要求加強對AI的監管。 法新社

等各方需要制定一套新的共同應對方案，做到發現漏洞後能更快處理。與此同時，專家警告指，黑客也會利用AI尋找漏洞，導致網絡攻擊風險上升。

專家指出，隨著前沿AI模型的能力不斷增強，其「雙刃劍」效應日益凸顯。現有前沿AI模型已具備持續實施複雜網絡攻擊的能力，黑客亦可借助AI批量自動掃描全球網絡脆弱節點，使網絡攻擊呈現「自動化、規模化、精準化」趨勢。

另一方面，AI擅長大規模數據分析、模式識別和自動監測，可協助網絡安全，使防禦方受益。使用AI協同識別和發現漏洞已成為業界普遍做法。蘋果早前所發布操作系統更新中的安全修復數量約為先前更新的5倍。該公司表示，其中多個漏洞由AI工具幫助識別。

《金融時報》此前報道說，AI正在迅速重塑網絡安全領域的攻擊和防禦模式，如何充分利用AI來提高網絡防禦能力成為新的挑戰。

負面新聞纏身 OpenAI上市前景添變數

【大公報訊】綜合路透社、《紐約時報》報道：美國人工智能（AI）巨頭OpenAI在推進首次公開募股（IPO）籌備期間，接連遭遇內部安全風波及財務不及預期等挑戰。隨着公眾對AI安全風險的擔憂攀升、監管加碼，多重矛盾令市場質疑其逾萬億美元的估值目標，上市進程蒙上陰影。該公司此前已表示不會在今年內上市。

今年7月，由OpenAI模型驅動的智能體在網絡安全評測中，利用漏洞突破隔離環境並侵入美國「抱抱臉」公司系統，引發全球對前沿AI安全問題的關注。此後，美國科企接連曝出AI模型和智能體失控相關問題，OpenAI多次暫停其最先進模型的訓練。

OpenAI商業盈利能力亦遭質疑。《金融時報》本月8日披露，OpenAI向投資者提交的數據顯示，公司截至9月底的年化營收「接近500億美元」，遠低於此前市場預期的700億美元。這一巨大差距讓投資者再次質疑其巨額AI基礎設施投入能否轉化為實質商業回報，打擊了資本市場的信心。

AI頻繁失控與科企財務狀況不理想，令美國民眾對AI的不信任感急升。近期民調顯示，高達四分之三的美國人認為，科企在防範AI對社會造成嚴重危害方面「做得遠遠不夠」。外界分析指出，若OpenAI無法有效化解安全與財務危機，其上市進程恐進一步被拖累。

Meta因誤導用戶被罰1950億

【大公報訊】綜合美國Axios新聞網、《衛報》報道：美國新墨西哥州一名法官21日裁定，美國科技巨頭、Facebook母公司Meta應就數據隱私誤導用戶問題繳納250億美元（約1950億港元）罰金。這一案件源自英國劍橋分析公司約10年前為時任美國共和黨總統候選人特朗普提供政治諮詢時，未經允許獲取數千萬Facebook用戶數據。

劍橋分析公司被曝在2016年美國總統選舉期間，經由第三方應用程序採集多達8700

萬Facebook用戶的個人數據。新墨西哥州檢方指控Meta向該州用戶撒謊，涉及誰能獲取他們的數據、Meta如何處理仇恨言論和虛假信息等問題。陪審團上月認定Meta誤導用戶，並且「故意違反」該州消費者保護法律總計近4390萬次。

法官馬修表示，以相關違法行為單次罰金最高5000美元計算，Meta本應繳納近2195億美元罰金，但他最終決定將罰金數額減至250億美元。他指出，第三方應用程序

開發者經由Facebook平台可獲取用戶信息，而Meta行政總裁朱克伯格在明知用戶不清楚該數據隱私漏洞的情況下利用了這一點。

美媒表示，這一案件說明，美國科技巨頭若在隱私問題上誤導用戶，將面臨重大財務後果。Meta首席法務官馬奧尼21日發表聲明稱，馬修的裁決和新墨西哥州檢方的執法手段「令在該州經商變得幾乎不可能」，並表示「確信將贏得上訴」。



上發表演講。 9月23日在Meta年度開發者大會 美聯社