檔　　號：
保存年限：

國立中山大學　書函

地址：804 高雄市鼓山區蓮海路70號
承辦人：施威志
電話：075252000#2521
電子信箱：wcs0503@mail.nsysu.edu.tw

受文者：如正副本

裝

發文日期：中華民國115年11月3日
發文字號：中圖資字第1151100146號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：為因應 PHP官方網站發布重大資安漏洞（CVE-2026-109618、CVE-2026-109619，外界稱 PHP2Shell），請各網站管理單位儘速完成清查、修補及相關防護措施，敬請轉知所屬知悉並配合辦理，請查照。

說明：

訂

一、依據 PHP 官方網站於2026年10月21日發布之安全公告，PHP 發布兩項重大安全漏洞，分別為 CVE-2026-109618及 CVE-2026-109619，CVSS v4.0 評分均為9.2（Critical）。攻擊者在特定條件下可能透過網路，在未經身分驗證的情況下執行任意程式碼，對網站伺服器及相關資訊系統造成重大資安風險。

二、本次漏洞影響所有對外提供 Web 服務之 PHP 網站，建請全校網站管理者採取下列措施：

(一)請立即清查委外或自建系統是否使用PHP程式環境。如為PHP環境，PHP官方已釋出8.5.12、8.4.27、8.3.36、8.2.35 安全更新，請協同委外廠商或各單位資訊人員，依系統環境儘速完成修補；使用 Linux 發行版或 LTS 廠商套件者，應確認並安裝供應商公告之已修補套件。如網站使用PHP8.1以下版本，請升級至8.2以上方可更新。

線

(二)更新後應確認實際執行版本，重新啟動 PHP及相關Web服務。另應加強監控網站存取紀錄、異常程序、可疑檔案、帳號及權限異動、對外連線與資安告警；未發現異常紀錄不代表系統未遭入侵。

(三)無法立即修補的系統，應優先參照PHP官方網站釋出之指引進行PHP相關參數的設定，採取初步防護措施，並

同時降低服務對外暴露面，視業務需求採取暫停服務、隔離系統、限制內部網路存取、VPN或IP白名單等措施。WAF及網路存取限制僅能作為防護參考，仍有可能面臨該漏洞所產生之重大資安風險與威脅，各單位應立即設定漏洞修補作業期限，儘速辦理PHP版本更新，以免產生後續重大危害。

(四)有關本案漏洞影響範圍、修補版本及暫時性緩解措施，請參閱：

１、ＰＨＰ　　官方網站安全公告：https://www.php.net/archive/2026.php#2026-10-21-5

２、政府相關資安機關之防護指引。

(１)https://www.twcert.org.tw/tw/cp-104-11308-ed8b8-1.html

(２)https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/Vulnerability_Alert_Announcements/5c4e9af1-4275-44ef-a277-c692786b5a2c/

三、如有相關問題，可洽詢本校圖書與資訊處資訊安全組或聯絡人施威志(分機2521)。

正本：本校各單位

副本：

依分層負責規定授權單位主管決行