

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2026102209102727	發佈時間	2026-10-22 09:24:28
事故類型	ANA-漏洞預警	發現時間	2026-10-22 09:24:28
影響等級	高		

[主旨說明:]【漏洞預警】PHP 存在高風險安全漏洞(CVE-2026-109618 與 CVE-2026-109619)，請儘速確認並進行處 置

[內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NICS-ANA-2026-0000952

研究人員發現 PHP 存在使用釋放後記憶體(Use After Free)漏洞(CVE-2026-109618 與 CVE-2026-109619)，攻擊者可透過傳送特製之 multipart/form-data HTTP 請求，於未經身分鑑別之情況下，於伺服器底層執行任意程式碼，網路上已出現本漏洞概念驗證程式(PoC)，請儘速確認並進行處置。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

已停止維護(EOL)之版本：

PHP 5.4.x 至 5.6.x 之所有版本

PHP 7.0.x 至 7.4.x 之所有版本

PHP 8.0.x 至 PHP 8.1.x 之所有版本

官方仍支援之版本：

PHP 8.5.11(含)以下版本

PHP 8.4.26(含)以下版本

PHP 8.3.35(含)以下版本

PHP 8.2.34(含)以下版本

註：WordPress、Drupal、Joomla 及 Magento 等內容管理系統之底層架構多使用 PHP 運

作，建議盤點與儘速進行處置。

[建議措施:]

官方將針對漏洞釋出修補或更新，建議系統管理者儘速將 PHP 升級至下列受支援之最新

安全版本：

PHP 8.5.12

PHP 8.4.27

PHP 8.3.36

PHP 8.2.35

官方更新公告與下載網址：

<https://www.php.net/downloads.php>

註：PHP 8.1(含)以下版本因官方已停止維護(EOL)，將不會獲得官方修補更新，建議儘速升級至上述仍支援之版本。

[參考資料:]

1. <https://nvd.nist.gov/vuln/detail/CVE-2026-109618>
2. <https://nvd.nist.gov/vuln/detail/CVE-2026-109619>
3. <https://www.php.net/archive/2026.php#2026-10-20-1>
4. <https://www.php.net/downloads.php>