

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2024061108062323	發佈時間	2024-06-11 08:24:25
事故類型	ANA-漏洞預警	發現時間	2024-06-07 21:58:25
影響等級	中		

[主旨說明:] **【漏洞預警】** PHP 存在高風險安全漏洞(CVE-2024-4577)，請儘速確認並進行修補！

[內容說明:]

轉發 國家資安資訊分享與分析中心 NISAC-200-202406-00000050

研究人員發現 PHP 存在引數注入(Argument Injection)漏洞(CVE-2024-4577)，未經身分鑑別之遠端攻擊者可透過特定字元序列繞過舊有 CVE-2012-1823 弱點修補後之保護，並透過引數注入等攻擊於遠端 PHP 伺服器上執行任意程式碼，請儘速確認並進行修補。

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」，煩請貴單位協助公告或轉發

[影響平台:]

- PHP 8.3 分支：8.3.8(不含)以下版本
- PHP 8.2 分支：8.2.20(不含)以下版本
- PHP 8.1 分支：8.1.29(不含)以下版本
- PHP 8.0 分支所有版本
- PHP 7 所有版本
- PHP 5 所有版本

[建議措施:]

官方已針對漏洞釋出修復更新，請更新至以下版本：

- PHP 8.3 分支請更新至 8.3.8(含)以上版本
- PHP 8.2 分支請更新至 8.2.20(含)以上版本
- PHP 8.1 分支請更新至 8.1.29(含)以上版本

針對 PHP 8.0、7 及 5 官方已不再維護，建議更換至仍在維護之版本

若無法更新 PHP，可參考以下緩解方式：

<https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/#1->

<https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/#2-%E5%B0%8D-xampp-for-windows-%E4%BD%BF%E7%94%A8%E8%80%85>

如使用 XAMPP for Windows 版本，可參考以下說明：

<https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/#2-%E5%B0%8D-xampp-for-windows-%E4%BD%BF%E7%94%A8%E8%80%85>

[參考資料:]

1. <https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/>