

張貼日期：2024/06/11

【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！

- 主旨說明：以Chromium為基礎之瀏覽器存在安全漏洞(CVE-2024-5274)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。
- 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：
 1. 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及7及5官方已不再維護，建議更換至仍在維護之版本
 2. 若無法更新PHP可參考以下緩解方式：<https://www.php.net/2024/06/01/advisory-2024-4577/>
 3. 如使用XAMPP for Windows版本，可參考以下說明：<https://www.php.net/2024/06/01/advisory-2024-4577/>
- 參考資料：
 - <https://devco.re/blog/2024/06/06/security-alert-cve-2024-4577-php-cgi-argument-injection-vulnerability/>

計算機與通訊中心
網路系統組 敬啟

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailing:announcement:20240611_01

Last update: 2024/06/11 16:04