

國家資通安全會報 國家資通安全科技中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2016-0074	發布時間	Mon Aug 01 09:41:37 CST 2016
事件類型	漏洞預警	發現時間	Thu Jul 21 00:00:00 CST 2016
警訊名稱	Apache 2.4.23(含)前的版本存在漏洞(CVE-2016-5387)，允許攻擊者遠端執行中間人攻擊，請儘速確認並進行修正		
內容說明	<p>Apache 伺服器是 Apache 軟體基金會旗下的一款 Web 伺服器，2.4.23(含)前的版本所內建之 httpd/mod_fcgid 等模組，其 HTTP_PROXY 環境變數未能有效過濾客戶端請求，造成 HTTP_PROXY 的變數內容，可被攻擊者發送的變數內容給覆蓋掉，造成攻擊者可利用此漏洞遠端執行中間人攻擊，以及將目標的 HTTP 流量重新導向至任意的伺服器。</p> <p>請各機關檢視是否安裝受影響之 Apache 伺服器，並儘速參考官方網頁所提供的臨時性解決方案進行修正。</p>		
影響平台	Apache 伺服器 2.4.23(含)前的版本		
影響等級	中		
建議措施	<p>請於已安裝 Apache 伺服器之電腦，使用「httpd -v」指令確認目前所使用之 Apache 版本，如所使用之 Apache 伺服器為 2.4.23(含)前的版本，請儘速依官方網頁(https://www.apache.org/security/asf-httpoxy-response.txt)所發布之臨時性解決方案進行修正，而現階段因官方尚未正式釋出修正後的版本，所以仍請各機關密切注意 Apache 官方網頁(http://httpd.apache.org/)的更新訊息。</p>		
參考資料	<p>1. https://httpoxy.org</p> <p>2. http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5387</p> <p>3. https://github.com/apache/httpd/commit/1c660f4f15083b06ce15018d304225c427973c26</p>		

此類通告發送對象為通報應變網站登記之資安人員。若貴單位之資安人員有變更，可逕自登入通報應變網站（<https://www.ncert.nat.gov.tw>）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號

聯絡電話： 02-27339922

傳真電話： 02-27331655

電子郵件信箱： service@nccst.nat.gov.tw