Apache Tomcat 伺服器 8.5.4(含)前的版本存在漏洞(CVE-2016-5388)，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：

Apache Tomcat是Apache軟體基金會旗下的一款輕量級Web伺服器，8.5.4(含)前的版本如啟用 CGI Servlet 執行 CGI 腳本(預設是關閉)，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。請檢視是否安裝受影響之 Apache Tomcat 伺服器，如啟用 CGI Servlet 執行 CGI 腳本，請儘速參考官方網頁所提供的臨時性解決方案進行修正。

影響平台：

Apache Tomcat 伺服器 8.5.4(含)前的版本

建議措施：

請於已安裝 Apache Tomcat 伺服器之電腦，依據不同平台使用「version.bat」或「version.sh」指令確認目前所使用之 Apache Tomcat

版本是否為 8.5.4(含)前的版本。

請於已安裝 Apache Tomcat 伺服器 8.5.4(含)前版本之電腦，檢視 conf/web.xml 設定檔，確認 Servlet 與 Servlet-mapping 區段是否為「註解」的狀態，若已「取消註解」，則表示已啟用 CGI Servlet 機制。

若已啟用 CGI Servlet 機制，且仍有使用之需求，目前可透過官方所發布之臨時性解決方案進行修正，例如重新編譯 tomcat/lib 目錄內的 catalina.jar 檔，或是自行編譯一個拒絕 PROXY Header 請求的 jar 檔等方法，詳細內容可參考官方網頁資訊 (https://www.apache.org/security/asf-httpoxy-response.txt)。現階段因官方尚未正式釋出修正後的版本，所以仍請密切注意 Apache Tomcat 官方網頁(http://tomcat.apache.org/)之更新訊息。

參考資料：

https://httpoxy.org

https://www.apache.org/security/

https://ci.apache.org/projects/tomcat/tomcat85/docs/apr.html

Publish Date

2016/7/21 0:00:00