若您收到這樣的訊息，

原發布編號	TWCERTCC-EWA-202303-0397	原發布時間	2023-03-27 12:30:08
事件類型	系統疑存在弱點	原發現時間	2023-03-22 16:55:33
事件主旨	臺北市大安區古亭國民小學設備IP：[redacted]等，Apache HTTP Server 疑似存在CVE 9.8資安漏洞，建議至少更新至最新版本		
事件描述	TWCERT/CC於近日接獲國際情資，發現 貴單位資訊設備IP[redacted]在 2023-03-22T16:55:33+0800 (UTC+0)期間，Apache HTTP Server 疑似存在CVE 9.8資安漏洞，Apache官方已針對這些漏洞釋出更新程式，建議至少更新至2.4.56(含)以上的版本。 Apache HTTP 伺服器存在CVE-2023-25690的漏洞，該漏洞的mod_proxy 配置允許 HTTP 請求走私攻擊，可能會導致繞過代理服務器中的訪問控制，並且將非預期的 URL 代理到現有的服務器。 受影響之 Apache HTTP Server 版本如下： 2.4.0 <= Apache HTTP Server <= 2.4.55 - CVE-2023-25690(HTTP請求不一致) 緩解措施： 1. 建議更新至Apache HTTP Server 2.4.56(含以上的版本) 2. 更新IBM的修補程式 3. 更新amazon linux的httpd、httpd24套件 參考資料： 1. https://nvd.nist.gov/vuln/detail/CVE-2023-25690 2. https://httpd.apache.org/security/vulnerabilities_24.html 3. https://www.ibm.com/support/pages/security-bulletin-ibm-http-server-vulnerable-http-request-splitting-due-included-apache-http-server-cve-2023-25690 4. https://alas.aws.amazon.com/cve/html/CVE-2023-25690.html 5. https://access.redhat.com/security/cve/cve-2023-25690 為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		

請按下步驟做Appache更新：

1.macOS開啟終端機

2.先查詢目前版本

httpd –v

會顯示目前版本

```
mdm:~ hhjh$ httpd -v
Server version: Apache/2.4.46 (Unix)
Server built:   Dec 21 2020 18:03:44
mdm:~ hhjh$
```

3.安裝brew 語法

/bin/bash –c "$(curl –fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"

系統會請您輸入管理員的密碼（也就是本機密碼）

等安裝好後

4.重新安裝Apache最新版

brew install httpd

等安裝好後

5.再次檢查版本
httpd –v

```
admin@mac ~ % httpd -v
Server version: Apache/2.4.56 (Unix)
Server built:   Mar  7 2023 18:18:55
admin@mac ~ %
admin@mac ~ %
```

就會是當下最新的版本
表示已完成 。

如果還是顯示舊版本，請將電腦重新開機，

重複第五點 ，再查詢一次，就會顯示正確囉。