張貼日期：2021/04/13

【資安漏洞預警Moodle數位學習平台疑似存在系統漏洞，請儘速確認並進行更新！

- 主旨說明：【資安漏洞預警Moodle數位學習平台疑似存在系統漏洞，請儘速確認並進行更新！

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202104-0468
  - 根據外部情資顯示，資安研究專家於2020年10月發現Moodle數位學習平台存在儲存式跨網站指令碼(Stored XSS)漏洞，漏洞編號為CVE-2021-20186造成該漏洞原因為Moodle TeX功能未做資料輸入驗證，駭客可透過此漏洞將惡意程式注入課程討論區，當使用者點選課程討論文章便觸發惡意程式，根據資安研究專家測試，此漏洞可造成課程成員個人資訊洩漏、權限提權及課程成績竄改等。
  - Moodle官方已於2021年1月釋出安全性更新版本，包含Moodle 3.10.1、3.9.4、3.8.7及3.5.16，相關安全性更新版本至少需使用PHP 7.0以上版本，技服中心發現部分TANET用戶PHP版本低於7.0版，相關Moodle對應PHP版本如下：
    - Moodle 3.10.1對應PHP版本至少7.2以上
    - Moodle 3.9.4對應PHP版本至少7.2以上
    - Moodle 3.8.7對應PHP版本至少7.1以上
    - Moodle 3.5.16對應PHP版本至少7.0以上
  - 建議TANET用戶比對Moodle版本是否屬已知漏洞之平台。
- 影響平台：
  - Moodle 3.10(含)
  - Moodle 3.9(含)至3.9.3(含)
  - Moodle 3.8(含)至3.8.6(含)
  - Moodle 3.5(含)至3.5.15(含) 其他更舊版本
- 建議措施：
  1. 檢視相關資訊設備是否屬已知漏洞之平台。
  2. 建議貴單位盤點內部是否存在相關Moodle平台，並檢視是否開啟TeX功能。
  3. 官方已釋出安全性更新版本，建議貴單位內部評估影響範圍與更新之必要性。
- 參考資料：
  1. [Moodle官方漏洞說明]https://moodle.org/mod/forum/discuss.php?d=417170
  2. [CVE-2021-20186漏洞說明]https://nvd.nist.gov/vuln/detail/CVE-2021-20186
  3. [漏洞資安報告]https://www.wizcase.com/blog/moodle-vulnerability-research/
  4. [OWASP Stored XSS說明]https://owasp.org/www-community/attacks/xss/

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:20210413_03

Last update: **2021/04/13 16:54**