張貼日期：2018/11/27

[資安漏洞預警通知] 電子學習平台Moodle出現嚴重CSRF缺陷，請儘速確認並進行修正

主旨：[資安漏洞預警通知] 電子學習平台Moodle出現嚴重CSRF缺陷，請儘速確認並進行修正

- 內容說明:
  - 開源電子學習平臺Moodle出現跨站請求偽造漏洞，能讓使用者身分驗證後與Moodle連線的期間，被有心人士冒名操作。
  - 這項弱點來自Moodle登入表單的安全機制，伺服器端透過authenticate_user_login( )函數，驗證使用者的請求是否合法，同時也可以一併檢查位於..\core\session\manager路徑之Token。不過，這項功能預設並未啟動。而外掛驗證工具或是內建的密碼變更模組執行時，上述的函數驗證請求的效力仍在，但缺乏Token檢驗，因此若是攻擊者加入新的組態參數$CFG→disablelogintoken就能製造跨站請求偽造攻擊，迴避Moodle對所有表單內的Token內容偵測。
  - 煩請各單位盡速確認是否使用該軟體，並進行版本更新以修補漏洞。
- 影響平臺：
  - Moodle 3.5.2以前版本
  - Moodle 3.4.5以前版本
  - Moodle 3.3.8以前版本
  - Moodle 3.1.14以前版本
- 建議措施：
  - 下載Moodle 3.6、3.5.3、3.4.6、3.3.9、3.1.15等修補版
- 參考資料：
  1. https://moodle.org/mod/forum/discuss.php?d=378731
  2. http://git.moodle.org/gw?p=moodle.git
  3. https://www.auscert.org.au/bulletins/72006
  4. https://securitytracker.com/id/1042154
  5. https://zh.wikipedia.org/wiki/%25E8%25B7%25A8%25E7%25AB%2599%25E8%25AF%25B7%25E6%25B1%2582%25E4%25BC%25AA%25E9%2580%25A0
  6. https://zh.wikipedia.org/wiki/Moodle
  7. https://itw01.com/FRIYWES.html
  8. http://git.moodle.org/gw?p=moodle.git&a=search&h=HEAD&st=commit&s=MDL-63183
  9. http://git.moodle.org/gw?p=moodle.git
  10. http://git.moodle.org/gw?p=moodle.git
  11. http://www.firnbergschulen.at/wp-content/uploads/2016/09/moodle-banner.png
  12. https://www.ithome.com.tw/news/127237?fbclid=IwAR31AHltI7sITzvckc49GOh6qqZqLWO-5VsgL3XybeVqwoHaEs6cnAm0GK0

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:20181127_01

Last update: **2018/11/27 11:13**