行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2017-0034	發布時間	Thu Mar 23 14:19:46 CST 2017
事件類型	漏洞預警	發現時間	Tue Mar 21 00:00:00 CST 2017
警訊名稱	特定版本 Moodle 平台存在 PHP 物件注入(Object Injection)弱點(CVE-2017-2641)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行修正		
內容說明	Moodle(Modular Object-Oriented Dynamic Learning Environment，模組化物件導向動態學習環境)是一款開放原始碼的學習與課程管理系統，由澳洲 Martin Dougiamas 採用 PHP 語言所設計開發的 Web-Based 應用系統，透過瀏覽器就可以輕鬆管理使用者、建構課程及豐富教學活動，應用在課程教學活動、員工教育訓練及學生遠距教學等。 該漏洞主要是 Moodle 程式碼內 grade_item 類別中的 update 方法(method)存在物件注入(Object Injection)弱點，導致攻擊者可藉由該弱點執行 SQL 注入獲取系統管理者權限，造成攻擊者可遠端執行任意程式碼，進而可能導致機敏資訊外洩等風險。		
影響平台	Moodle 3.2 至 3.2.1(含)版本 Moodle 3.1 至 3.1.4(含)版本 Moodle 3.0 至 3.0.8(含)版本 Moodle 2.7.0 至 2.7.18(含)版本 其他已不支援版本		
影響等級	中		
建議措施	檢視 Moodle 版本，方法有以下兩種： 1. 檢視 Moodle 根目錄下之 version.php 檔 2. 若為 Moodle 管理者可直接在設定 Setting->Site administration->Notifications 中檢視 Moodle 版本 如所使用的 Moodle 版本為上述(3.2 至 3.2.1、3.1 至 3.1.4、3.0 至 3.0.8、2.7.		

	0 至 2.7.18 或已不支援)受影響之版本，請更新官方網頁所釋出最新之 Moodle 3.2.2、3.1.5、3.0.9 或 2.7.19 版本。
參考資料	1.http://netanelrub.in/2017/03/20/moodle-remote-code-execution/ 2.https://download.moodle.org/ 3.https://download.moodle.org/releases/legacy/

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