張貼日期：2019/02/25

[資安漏洞預警通知] Drupal存在安全漏洞(CVE-2019-6340)允許攻擊者遠端執行任意程式碼，請盡速確認並進行更新

主旨：[資安漏洞預警通知] Drupal存在安全漏洞(CVE-2019-6340)允許攻擊者遠端執行任意程式碼，請盡速確認並進行更新

- 內容說明:
  - Drupal是一個開源且以PHP語言寫成的內容管理框架(CMF)
  - 研究人員發現Drupal存在安全漏洞(CVE-2019-6340)當攻擊者以PATCH或POST方式傳送RESTful Web資料時Drupal並未對資料進行嚴格的檢查，進而導致執行任意PHP程式碼。
- 影響平台:

1. 有啟用RESTful Web Services模組，且接受PATCH或POST請求的網站
2. 使用JSON:API模組的網站
3. Drupal 7使用RESTful Web Services或Services模組的網站

- 建議措施:
  1. 版本更新：可於CHANGELOG.txt檔案進行版本確認。
     - 若使用Drupal 8.6.x版本，需升級至Drupal 8.6.10以後版本：https://www.drupal.org/project/drupal/releases/8.6.10
     - 若使用Drupal 8.5.x(含)以前版本，需升級至Drupal 8.5.11以後版本：https://www.drupal.org/project/drupal/releases/8.5.11&
  2. 模組更新：更新網址https://www.drupal.org/security/contrib
     - 用Drupal 8版本更新後，須再更新受影響模組之安全性更新，受影響模組如下：
       - JSON:API
       - Metatag
       - Video
       - Paragraphs
       - Translation Management Tool
       - Font Awesome Icons
  3. 使用Drupal 7不需進行版本升級，但部分受影響模組需進行更新，受影響模組如下：
     - RESTful Web Services
     - Link
  4. 請定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為，亦須更新防毒軟體病毒碼以加強防護
- 參考資料:
  1. https://www.drupal.org/sa-core-2019-003
  2. https://www.tenable.com/blog/highly-critical-drupal-security-advisory-released-sa-core-2019-003
  3. https://thehackernews.com/2019/02/hacking-drupal-vulnerability.html

---

計算機與通訊中心

網路系統組 敬啟