

# 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-2019-0021	發布時間	Sat Feb 23 09:17:16 CST 2019
事件類型	漏洞預警	發現時間	Fri Feb 22 00:00:00 CST 2019
警訊名稱	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	<p>Drupal 是一個開源且以 PHP 語言寫成的內容管理框架(CMF)</p> <p>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</p>		
影響平台	<p>?Drupal 8：</p> <ol style="list-style-type: none"> <li>1. 有啟用 RESTful Web Services 模組，且接受 PATCH 或 POST 請求的網站</li> <li>2. 使用 JSON:API 模組的網站</li> </ol> <p>?Drupal 7：使用 RESTful Web Services 或 Services 模組的網站</p>		
影響等級	高		
建議措施	<p>版本更新：可於 CHANGELOG.txt 檔案進行版本確認。</p> <p>?若使用 Drupal 8.6.x 版本，需升級至 Drupal 8.6.10 以後版本：<a href="https://www.drupal.org/project/drupal/releases/8.6.10">https://www.drupal.org/project/drupal/releases/8.6.10</a></p> <p>?若使用 Drupal 8.5.x(含)以前版本，需升級至 Drupal 8.5.11 以後版本：<a href="https://www.drupal.org/project/drupal/releases/8.5.11">https://www.drupal.org/project/drupal/releases/8.5.11</a></p> <p>模組更新：更新網址 <a href="https://www.drupal.org/security/contrib">https://www.drupal.org/security/contrib</a>。</p> <p>?使用 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：</p>		

\* JSON:API

\* Metatag

\* Video

\* Paragraphs

\* Translation Management Tool

\* Font Awesome Icons

?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

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>

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@ncst.nat.gov.tw](mailto:service@ncst.nat.gov.tw)

