張貼日期：2025/07/16

【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/07/07-2025/07/13)

- 主旨說明:【漏洞預警】CISA新增5個已知遭駭客利用之漏洞至KEV目錄(2025/07/07-2025/07/13)

- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202507-00000010

1. 【CVE-2019-9621】Synacor Zimbra Collaboration Suite (ZCS) Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 Synacor Zimbra Collaboration Suite存在透過ProxyServlet元件實現的伺服器端請求偽造漏洞。
   - 【影響平台】請參考官方所列的影響版本
   - https://blog.zimbra.com/2019/05/9826/
2. 【CVE-2019-5418】Rails Ruby on Rails Path Traversal Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 Rails Ruby on Rails在Action View存在路徑漏洞。結合特製的Accept標頭與對render file:的呼叫，可能導致目標伺服器上任意檔案的內容被洩漏。
   - 【影響平台】請參考官方所列的影響版本
   - https://web.archive.org/web/20190313201629/https://weblog.rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released/
3. 【CVE-2016-10033】PHPMailer Command Injection Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 PHPMailer存在指令注入漏洞，原因是未能適當處理使用者提供的輸入。攻擊者可利用此漏洞在應用程式的上下文中執行任意程式碼，若嘗試攻擊失敗會導致阻斷服務。
   - 【影響平台】請參考官方所列的影響版本
   - https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities
4. 【CVE-2014-3931】Multi-Router Looking Glass (MRLG) Buffer Overflow Vulnerability (CVSS v3.1: 9.8)
   - 【是否遭勒索軟體利用:未知】 Multi-Router Looking Glass存在緩衝區溢位漏洞，遠端攻擊者可藉此導致任意記憶體寫入及記憶體損毀。
   - 【影響平台】請參考官方所列的影響版本
   - https://mrlg.op-sec.us/
5. 【CVE-2025-5777】Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability (CVSS v3.1: 7.5)
   - 【是否遭勒索軟體利用:未知】 Citrix NetScaler ADC和Gateway存在因輸入驗證不足而導致的越界讀取漏洞。當NetScaler 被配置為Gateway(VPN 虛擬伺服器、ICA Proxy、CVPN、RDP Proxy)或AAA虛擬伺服器時，該漏洞可能導致記憶體過讀讀取。
   - 【影響平台】請參考官方所列的影響版本
   - https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

- 影響平台:
  - 詳細內容於內容說明欄之影響平台
- 建議措施:

1. 【CVE-2019-9621】 官方已針對漏洞釋出修復更新，請更新至相關版本
   - https://blog.zimbra.com/2019/05/9826/

2. CVE-2019-5418 官方已針對漏洞釋出修復更新，請更新至相關版本
   https://web.archive.org/web/20190313201629/https://weblog.rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released/
3. CVE-2016-10033 官方已針對漏洞釋出修復更新，請更新至相關版本
   - https://github.com/PHPMailer/PHPMailer/wiki/About-the-CVE-2016-10033-and-CVE-2016-10045-vulnerabilities
4. CVE-2014-3931 官方已針對漏洞釋出修復更新，請更新至相關版本
   - https://mrlg.op-sec.us/
5. CVE-2025-5777 官方已針對漏洞釋出修復更新，請更新至相關版本
   - https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

計算機與通訊中心
網路系統組 敬啟