張貼日期：2026/07/16

【漏洞預警】Splunk Enterprise、Splunk Cloud Platform及Splunk Secure Gateway存在高風險安全漏洞(CVE-2026-20251)，請儘速確認並進行修補

- 主旨說明:【漏洞預警】Splunk Enterprise、Splunk Cloud Platform及Splunk Secure Gateway存在高風險安全漏洞(CVE-2026-20251)，請儘速確認並進行修補

- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-200-202607-00000001
  - 研究人員發現Splunk Enterprise、Splunk Cloud Platform及Splunk Secure Gateway存在不安全之反序列化(Insecure Deserialization)漏洞(CVE-2026-20251)，已通過身分鑑別之遠端攻擊者可透過對未受信任之資料進行反序列化，進而於受影響伺服器上執行任意程式碼，請儘速確認並進行修補。
- 影響平台:
  - Splunk Enterprise 10.2.0至10.2.3版本
  - Splunk Enterprise 10.0.0至10.0.6版本
  - Splunk Enterprise 9.4.0至9.4.11版本
  - Splunk Enterprise 9.3.0至9.3.12版本
  - Splunk Cloud Platform 10.3.2512.12(不含)以前版本
  - Splunk Cloud Platform 10.2.2510.14(不含)以前版本
  - Splunk Cloud Platform 10.1.2507.22(不含)以前版本
  - Splunk Cloud Platform 9.3.2411.132(不含)以前版本
  - Splunk Secure Gateway 3.10.6(不含)以前版本
  - Splunk Secure Gateway 3.9.20(不含)以前版本
  - Splunk Secure Gateway 3.8.67(不含)以前版本
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：https://advisory.splunk.com/advisories/SVD-2026-0601
- 參考資料:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-20251
  2. https://advisory.splunk.com/advisories/SVD-2026-0601

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:20260716_22

Last update: **2026/07/16 15:39**