美國國家安全局發布「軟體記憶體安全須知」

美國國家安全局（National Security Agency, NSA）於2022年11月10日發布「軟體記憶體安全須知」（“Software Memory Safety” Cybersecurity Information Sheet），說明目前近70%之漏洞係因記憶體安全問題所致，為協助開發者預防記憶體安全問題與提升安全性，NSA提出具體建議如下：

1.使用可保障記憶體安全之程式語言（Memory safe languages）：建議使用C#、Go、Java、Ruby、Rust與Swift等可自動管理記憶體之程式語言，以取代C與C++等無法保障記憶體安全之程式語言。

2.進行安全測試強化應用程式安全：建議使用靜態（Static Application Security Testing, SAST）與動態（Dynamic Application Security Testing, DAST）安全測試等多種工具，增加發現記憶體使用與記憶體流失等問題的機會。

3.強化弱點攻擊防護措施（Anti-exploitation features）：重視編譯（Compilation）與執行（Execution）之環境，以及利用控制流程防護（Control Flow Guard, CFG）、位址空間組態隨機載入（Address space layout randomization, ASLR）與資料執行防護（Data Execution Prevention, DEP）等措施均有助於降低漏洞被利用的機率。

搭配多種積極措施增加安全性：縱使使用可保障記憶體安全之程式語言，亦無法完全避免風險，因此建議再搭配編譯器選項（Compiler option）、工具分析及作業系統配置等措施增加安全性。

相關連結

NSA Releases Guidance on How to Protect Against Software Memory Safety Issues, National Security Agency

你可能會想參加

- → 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- → 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- → 供應鏈資安國際法制與政策趨勢分享會
- → 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- → 商業服務業個資保護宣導說明會
- → 【實體】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 【直播】2024科技研發法制推廣活動— 科專個資及反詐騙實務講座
- → 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

鄭岱宜
副法律研究員 編譯整理

上稿時間： 2023年03月

資料來源：

NSA Releases Guidance on How to Protect Against Software Memory Safety Issues, National Security Agency, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3215760/nsa-releases-guidance-on-how-to-protect-against-software-memory-safety-issues/ (last visited Jan. 30, 2023).

延伸閱讀：

阮韻蒨，〈美國公布實施零信任架構相關資安實務指引〉，科技法律研究所，2022/09，https://stli.iii.org.tw/article-detail.aspx?tp=1&d=8885&no=64（最後瀏覽日：2023/01/30）。

文章標籤

推薦文章