SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

2026 年 6 月 2 日

致持牌法團、獲證監會發牌的虛擬資產服務提供者及有聯繫實體的通函

加強網絡安全措施　應對人工智能驅動的網絡攻擊引發的新興風險

1. 隨著網絡威脅形勢不斷演變，香港網絡安全事故數目日漸增加[1]，前沿人工智能（artificial intelligence，簡稱 AI）模型帶來的網絡攻擊風險亦見升溫。有鑑於此，證券及期貨事務監察委員會（證監會）謹此提醒持牌法團、獲證監會發牌的虛擬資產服務提供者及其有聯繫實體（統稱“持牌機構”），應檢視並加強各自的網絡安全措施，以應對這些不斷演變的威脅。

2. 證監會一直與持牌機構及主要網上交易平台營運者保持溝通，了解機構是否已準備好應對可能由 AI 驅動工具輔助或加速發動的網絡攻擊。本通函闡述證監會在溝通過程中的觀察所得，並提供實用指引，以協助持牌機構加強抵禦風險的能力和對策。

3. 持牌機構應評估其是否已準備好應對 AI 驅動的網絡攻擊，並採取適當行動以處理其現行系統中的任何漏洞，同時加強網絡安全措施，從而更妥善地保障自身營運和保護客戶利益。持牌機構應注意，其高級管理層（包括負責資訊科技職能的核心職能主管）須就他們所屬機構的網絡安全風險管理，負上最終責任。尤其是，負責資訊科技職能的核心職能主管應確保，對機構網絡安全框架作出的改動均經充分審視及批准，並確保對機構網絡安全措施作出的優化安排及時妥為執行。如有需要，持牌機構應向資訊科技安全專家徵詢意見及尋求協助。

AI 驅動的網絡威脅的新形勢

4. AI 能力的新近發展，可大幅減低識別並利用關鍵軟件及基建漏洞所需的專業知識、成本及時間。持牌機構尤應注意以下發展：

- *網絡攻擊的複雜程度及頻率日增*：前沿 AI 模型現正迅速演進，展現出前所未見的能力 — 自主策劃並執行涉及多個步驟的複雜行動。舉例來說，該等模型愈來愈能識別出迄今尚未被軟件開發人員發現的安全漏洞（俗稱“零日漏洞”）。它們亦能有系統地識別出多項“風險評級較低”的漏洞[2]，並將之串連起來加以利用，從而對系統造成重大干擾。此外，它們可在多個互聯系統之間跨系統運作，並策動大規模攻擊。

  AI 驅動工具的普及，亦可能大幅降低威脅者執行各類惡意活動的技術門檻，例如網絡釣魚、社交工程、深度偽造假冒他人身分及偵察。

  這些發展為潛在網絡攻擊的速度和規模增添了新維度，而持牌機構、其員工及客戶料將受到更頻密且更具針對性的攻擊。因此，持牌機構應檢視其現有的網絡攻擊預防、偵測、應對及復原程序是否仍然有效。

---

1 香港網絡安全事故協調中心的資料顯示，網絡安全事故數目（包括殭屍網絡、分散式阻斷服務、塗改攻擊、惡意程式及網絡釣魚由 2024 年的 12,536 宗增至 2025 年的 15,877 宗。

2 “風險評級較低”的漏洞指若被利用會對有關機構造成輕微影響的漏洞。

- *採取補救措施以減低潛在網絡攻擊風險的應變時間已見縮短*：低成本 AI 驅動工具日漸普及，有助迅速識別新漏洞。主要軟件供應商發布的安全修補程式及更新在數量和頻率上料會明顯增加。此外，隨著這些 AI 工具的出現，由漏洞被識別或披露至被威脅者利用之間的時間間隔正迅速縮短。

  修補及變更管理程序一般涉及多個步驟，包括與軟件供應商協調、測試、部署及檢討，均需時完成。因此，持牌機構應加強並加快其修補及漏洞管理程序，以盡量縮小面對潛在攻擊的風險敞口。

應對 AI 驅動的網絡攻擊潛在風險的措施

5. 持牌機構應實施穩健的安全監控措施並適時作出更新，以保護其系統免受潛在威脅，防止客戶機密資料遭到未經授權的接達或披露，以及保障客戶資產免因網絡攻擊而被挪用。

6. 作為基礎，持牌機構應就其科技資產及組件（包括硬件、軟件、網絡基建、數據庫及雲端服務）備存一份準確且持續更新的清單。持牌機構應識別哪些資產及服務屬對外暴露、對業務至為關鍵（統稱“業務關鍵組件”），或須倚賴第三方組件，以便能迅速而有效地將補救及保護措施集中於最高風險範疇。此外，鑑於前沿 AI 模型能以極快速度識別出可被利用的弱點，持牌機構應確保其資產清單保持充分更新，以便在出現新漏洞或威脅情報時，可即日決定各項工作的緩急優次及控制損毀的安排。

7. 鑑於各種漏洞現時可更迅速地被識別出來並被人加以利用，持牌機構應檢討並加強其網絡安全框架，確保該等框架在預防、偵測、應對及復原方面仍屬合適及有效，以抵禦不斷演變的威脅。持牌機構在檢討及加強其框架時，應考慮下文(A)至(E)各節所述的範疇。附錄列出一些監控措施及程序的示例，旨在協助持牌機構管理及紓減與 AI 驅動的網絡攻擊相關的潛在風險。

8. 此外，持牌機構應注意，在業務運作中使用 AI 語言模型（不論有關模型是否由內部開發、由集團公司或第三方服務提供者提供，或者取自開放來源），或會放大現有網絡風險和帶來額外風險，而這些額外風險可能在 AI 輔助發動的網絡攻擊期間被人利用或觸發，當中包括因針對 AI 語言模型的對抗性攻擊、數據洩露及系統提示被推翻而引起的風險。因此，持牌機構應確保其網絡安全框架及事故處理安排已就有關網絡安全風險制訂對策，並考慮《2024 年 11 月通函》[3]所列出的核心原則。另外，持牌機構如擬在高風險用例[4]中採用 AI 語言模型，應注意其有責任遵守《證券及期貨（發牌及註冊）（資料）規則》下的通知規定[5]。

(A) 修補及漏洞管理

9. 持牌機構應檢視並加強其修補及漏洞管理程序。持牌機構應迅速採取行動處理已知漏洞，並就處理超出例行修補周期的緊急及重要修正程式制訂適當的政策和程序，尤其是針對影響其

---

3 日期為 2024 年 11 月 12 日的《致持牌法團的通函 — 生成式 AI 語言模型的使用》（《2024 年 11 月通函》）。

4 《2024 年 11 月通函》第 8 段。

5 《2024 年 11 月通函》第 30 段。

業務關鍵組件的漏洞和修正程式。持牌機構亦應分配足夠資源，務求有效地應付修補需求可能急增的情況。

(B) 接達及權限監控措施

10. 持牌機構設計系統監控措施時，應基於任何使用者、裝置、高權限帳戶或網絡組件均可被入侵[6]的假設。尤其是，持牌機構應實施穩健的接達及權限監控措施，並盡量將攻擊面減至最低。

11. 為減低不受信任的輸入內容或未經授權的使用者可能操控系統或工作流程的風險，持牌機構應：

    (i) 對所有業務關鍵組件的接達執行最小權限原則，包括將連接器及工具權限限制在預定用例所需的必要範圍內，並實施適當措施保障高權限帳戶[7]；

    (ii) 加強防火牆及網絡分段。尤其是，持牌機構應在可行的情況下實施微網絡分段，以限制在網絡和系統之間橫向移動的能力；

    (iii) 將外部及不受信任的輸入內容（包括從應用程式、電郵、文件及網頁擷取的內容）視為可能具對抗性的內容，並防止該等輸入內容直接更改系統指示或觸發高權限操作；及

    (iv) 就影響巨大的操作實施輸入與核對的分工監控措施。

(C) 偵測及監察措施

12. 持牌機構應加強其威脅偵測及對客戶交易活動和系統活動中的異常情況的監察，以確保該等措施與不斷演變的威脅環境相稱。持牌機構亦應提升其收集威脅情報的能力。

(D) 第三方供應鏈風險管理

13. 持牌機構應實施妥善程序，以應付針對支援其關鍵運作和業務關鍵組件的第三方服務提供者（第三方服務提供者）的 AI 驅動威脅。持牌機構應加強其第三方供應鏈風險管治框架，優化對第三方服務提供者的初步和持續評估，以納入最新的威脅形勢，並確保妥善管理與第三方服務提供者相關的網絡安全風險，尤其是 AI 驅動的網絡攻擊所產生的風險。

---

6 採用此設計原則的網絡可稱為“零信任網絡”，而在該網絡下，不會單憑網絡位置或使用者身分而默認任何接達為受信任。

7 這指擁有較高權限的帳戶，准許使用者接達持牌機構的網絡、系統、伺服器及裝置，並可（其中包括）改動系統配置、管理其他使用者帳戶及帳戶權限，以及修改客戶資料。

(E) 事故應對及復原

14. 持牌機構應檢視並優化其網絡安全事故處理程序及應變計劃，以有效地應對 AI 驅動的網絡攻擊，而該等攻擊或會導致其網絡和系統遭未經授權接達、敏感資料外洩，以及服務受到嚴重干擾等情況。

15. 持牌機構應意識到，傳統偵測與應對程序的處事速率可能跟不上 AI 驅動的攻擊速度。因此，若然單靠在發生事故後進行調查或透過正常渠道上報問題，直至採取有效行動之前，有關攻擊或會持續發酵，且有關情況亦有可能惡化下去。因此，持牌機構應設立適當的上報及匯報機制，並考慮預先計劃的控制損毀及阻斷漏洞利用策略，包括迅速封鎖惡意活動、隔離受影響系統及限制接達的能力。

16. 持牌機構應定期透過桌面演練、模擬攻擊或其他適當方式，測試其網絡安全事故處理程序及應變計劃，以評估相關程序和計劃的成效。

17. 持牌機構應定期備存[8]業務紀錄、客戶和交易數據庫以及證明文件，並實施適當措施確保備份的副本可供使用。

18. 持牌機構亦應按照《操守準則》[9]及《虛擬資產交易平台指引》[10]的規定，及時向證監會報告重大網絡安全事故和攻擊。

未來路向

19. 證監會將會繼續密切監察此範疇的最新發展，並與業界、主要科技服務提供者及其他監管機構保持緊密溝通。鑑於風險不斷演變，證監會在適當情況下或會發出進一步指引，進行檢視以評估持牌機構在處理網絡安全事故方面的準備程度及應變能力，或採取監管行動。

20. 如對本通函有任何疑問，請聯絡你的個案主任。

證券及期貨事務監察委員會
中介機構部

連附件

完

SFO/IS/020/2026

---

8 從事電子交易的持牌法團（見《證券及期貨事務監察委員會持牌人或註冊人操守準則》（《操守準則》）第 18.2(d)段）及虛擬資產服務提供者，均須至少每日備存該等紀錄及數據。

9 《操守準則》第 12.5(e)段。

10 《適用於虛擬資產交易平台營運者的指引》（《虛擬資產交易平台指引》）第 16.7(b)及(c)段。