

親愛的客戶:

使用有安全更新的軟件和定期安裝保安修補程式

駭客會利用網絡安全漏洞來攻擊一些還未安裝修補程式的電腦，所以當軟件商發現軟件程式錯誤或出現安全風險時，便會向用戶提供一些修補程式去修補這些漏洞。

沒有及時更新修補程式引致的潛在保安風險

- 攻擊者有機會利用未有修補程式的過時軟件對電腦進行攻擊。
- 新版本的保安軟件可能無法完全兼容過時的操作系統，以致限制了對電腦系統的保護。
- 過時軟件安全標準的安全程度可能較低，容易遭受網絡攻擊。

減低風險的建議

- 移除過時軟件產品，或升級軟件產品以保證繼續有安全更新的支援。
- 為電腦系統進行保安強化，如移除不必要的軟件和服務。
- 大部分軟件商都會將最新保安漏洞的資料及修補程式放在他們的網站。請經常留意相關資訊，向供應商諮詢更新修補程式程序的步驟和及時安裝，並於下載修補程式的網頁添加書籤。
- 部份軟件商亦提供自動更新修補程式的功能。例如微軟視窗的自動更新功能，如被啟動的話，便能為你的電腦自動下載及安裝修補程式。
- 如果有需要在過渡時期使用過時的電腦系統，要先評估有關保安風險，並在使用前採取補救性保安措施。
- 在更新之前，請確保修補程式是來自信任的來源及已被測試。
- 修補程式程序應在所有級別進行更新，包括但不限於：
 1. 韌體
 2. OS 操作系統
 3. 驅動程式
 4. 終端用戶應用程式
 5. 功能和插件
- 注意跟軟件產品相關的保安新聞和資訊，並採取適當的應對措施，例如停止使用該產品。
- 採用可以繼續支援你的電腦系統的保安軟件。
- 盡可能使用普通權限帳戶工作，避免使用管理員權限帳戶，因為攻擊者通常使用已登入的用戶帳戶權限來執行惡意程式。
- 使用有安全更新的、最新及有支援的軟件、瀏覽器和插件。
- 避免在過時的電腦系統儲存敏感資料或進行涉及敏感性資料的活動，例如網上購物、操作股票交易或網上銀行服務等。

我司會不時更新關於網絡安全的提示，請您關注我司以下網站：

http://www.ssif.com.hk/main_hk/customerCenter/cybersecurity/index.shtml

如有垂詢，請聯絡您的客戶經理或致電客戶服務熱線 +852 2501 1001（香港及海外）或 +86 4008411618（中國內地）。

山證國際證券有限公司

山證國際期貨有限公司 謹啟

2022年8月16日