U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Privacy, Access, Civil Liberties, and Transparency
Washington, DC 20528

2024 年 6 月 20 日

尊敬的同事,

如**您所知，網絡安全和基礎設施安全局**（CISA）的化學品安全評估工具（CSAT）在 2024 年 1 月 23 日至 2024 年 1 月 26 日期間成為惡意行為者網絡安全入侵的目標，導致可能未經授權訪問人員擔保計劃提交的文件和化學恐怖主義脆弱性信息（CVI）授權用戶的賬戶。

雖然 CISA 的調查沒有發現這些數據被外泄的證據，但出於謹慎起見，我們還是通知了所有將個人身份信息 (PII) 提交給 CISA 的化學設施反恐標準 (CFATS) 計劃進行審查或擁有 CVI 授權用戶賬戶的個人，這些信息可能已被不當訪問。我和**你一樣感到擔憂和沮喪，並向你提供我們所知道的有關這次企圖入侵的信息。**

您收到此通知是因為（1）您曾進入限製區域和/或關鍵資產的化工設施，該設施可能已經向人員保障計劃提交了您的個人可識別信息進行審查，或者（2）您或化工設施在2007年6月至2023年7月期間提交了有限的個人可識別信息和商務聯系信息，以便創建CVI授權用戶賬戶。我們還聯系了您所在的化工廠，了解有關入侵的技術細節。

可能受到影響的信息

人員擔保計劃. CFATS 人員擔保計劃使受 CFATS 監管的設施能夠遵守基於風險的績效標準 (RBPS) 12(iv)--人員擔保。RBPS 第 12(iv)[1]條要求對已經或正在設法進入高風險化學設施禁區和重要資產的設施人員和無陪同訪客進行篩查，以確定他們是否與恐怖分子有潛在聯系。這包括通過 CSAT 提交 PII 以進行直接審查，或重新利用國土安全部其他計劃下進行的審查，以便根據恐怖分子篩查數據庫對個人進行審查[2]。

通過人事擔保計劃提交的個人信息包括個人姓名、出生日期、公民身份或性別。如果有或需要，還提供了非美國人的其他個人信息，包括：

- 別名
- 出生地
- 國籍
- 護照號碼
- 申訴編號

[1] 6 C.F.R. 27.230(a)(12(iv)。
[2] 有關恐怖分子篩查數據庫的更多信息，請訪問：https://www.fbi.gov/investigate/terrorism/tsc

- A 編號
- 全球入境 ID 編號
- TWIC ID 編號

CSAT 用戶帳號。一般來說，為設施提交CSAT信息的用戶賬戶有兩種類型：提交或參與開發頂層調查、安全漏洞評估和場地安全計劃（包括CVI授權用戶）的CSAT用戶，以及提交人員保障信息的CSAT用戶。在這兩種情況下，為創建 CSAT **賬**戶而收集的信息都是一樣的：姓名、職務、公司地址和公司電話號碼。

入侵詳情

1 月 26 日，CISA 發現了影響 CSAT Ivanti Connect Secure 設備的潛在惡意活動[3]。CISA 立即將系統下線，將應用程序與網絡的其他部分隔離，並開始進行取證調查。此次調查包括來自 CISA 首席信息官**辦公室、網絡安全部威脅獵殺小組和國土安全部網絡運行中心的技術專家。**

在調查過程中，我們發現惡意行為者在 Ivanti 設備上安裝了高級 webshell。這類 webshell 可用於執行惡意命令或向底層系統寫入文件。我們的分析進一**步發現，一名惡意行為者在兩天**內多次訪問了該 webshell。

重要的是，調查已經結束，並未發現 CSAT 數據泄露或 Ivanti 設備之外的對手訪問。CSAT 中的所有信息都使用 AES 256 加密技術進行加密，**每個應用程序的信息都有額外的安全控製措施，以限製橫向訪問的可能性。加密密鑰被隱藏，以防止威脅行為者對系統的訪問。**

為受影響的個人提出的建議

雖然 調查沒有發現憑證被盜的證據，但我們建議您閱讀並遵循 CISA 關於如何保護自己免受網絡行為者暴力攻**擊的指南**(https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), 選擇密碼並保護密碼 (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), 和多重身**份驗證** (https://www.cisa.gov/MFA).

CISA 創建了一個網站，提供本通知的副本、常見問題、定期更新以及註冊電子郵件發送列表以接收網站更新的機會。在 CISA 探索其他可能的補救措施的過程中，我們鼓勵**您註冊加入我們針對此事件的發布列表，以便接收** www.cisa.gov/csat-notification 上的所有最新更新。受影響的個人如對此事件有任何疑問，請發送電子郵件至 CFATS.Notificiations@cisa.dhs.gov 聯系 CISA 化學安全分部。

此致,

[3] 有關此類惡意活動的更多信息，請訪問：https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

詹姆斯-伯德
首席隱私官