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

June 20, 2024

Dear Colleague,

As you may know, the Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Security Assessment Tool (CSAT) was the target of a cybersecurity intrusion by a malicious actor from January 23, 2024 to January 26, 2024, which resulted in the potential unauthorized access of Personnel Surety Program submissions and accounts for Authorized Users of Chemical-terrorism Vulnerability Information (CVI).

While CISA's investigation found no evidence of exfiltration of this data, we are notifying all individuals who had their personally identifiable information (PII) submitted to CISA's Chemical Facility Anti-Terrorism Standards (CFATS) program for vetting or had a CVI Authorized User account out of an abundance of caution that this information could have been inappropriately accessed. I share your concern and frustration and am providing you with information we know about this attempted intrusion.

You are receiving this notification because (1) a chemical facility where you had access to restricted areas and/or critical assets may have submitted PII on you for vetting under the Personnel Surety Program or (2) you or a chemical facility submitted limited PII and business contact information for the creation of a CVI Authorized User account between the dates of June 2007 and July 2023. We have also reached out to the chemical facility that you are associated with regarding technical details about the intrusion.

Information Potentially Impacted

Personnel Surety Program. The CFATS Personnel Surety Program enabled CFATS-regulated facilities to comply with Risk-Based Performance Standard (RBPS) 12(iv) —Personnel Surety. RBPS 12(iv)[1] required facility personnel and unescorted visitors who had or were seeking access to restricted areas and critical assets at high-risk chemical facilities to be screened for potential terrorist ties. This included submitting PII through CSAT for direct vetting or repurposing vetting conducted under other Department of Homeland Security programs in order to vet individuals against the Terrorist Screening Database[2].

PII submitted through the Personnel Surety Program included an individual's name, date of birth, citizenship, or gender. Additional PII was provided, if available or required for a non-U.S. person, including:

- Aliases
- Place of Birth

[1] 6 C.F.R. 27.230(a)(12(iv).
[2] For more on the Terrorist Screening Database, visit: https://www.fbi.gov/investigate/terrorism/tsc

- Citizenship
- Passport Number
- Redress Number
- A Number
- Global Entry ID Number
- TWIC ID Number

CSAT User Accounts. In general, there are two types of user accounts for facilities submitting information for CSAT: CSAT users submitting or involved in the development of Top-Screen surveys, Security Vulnerability Assessments, and Site Security Plans (to include CVI authorized users) and CSAT users submitting personnel surety information. In both cases, the information collected for the creation of a CSAT account is the same: name, title, business address, and business phone number.

Details of the Intrusion

On January 26, CISA identified potentially malicious activity[3] affecting the CSAT Ivanti Connect Secure appliance. CISA immediately took the system offline, isolated the application from the rest of the network, and began a forensic investigation. This investigation included technical experts from CISA's Office of the Chief Information Officer, our Cybersecurity Division's Threat Hunting team, and the Department of Homeland Security's Network Operations Center.

During the investigation, we identified that a malicious actor installed an advanced webshell on the Ivanti device. This type of webshell can be used to execute malicious commands or write files to the underlying system. Our analysis further identified that a malicious actor accessed the webshell several times over a two-day period.

Importantly, the investigation has concluded and did not identify exfiltration of data from CSAT or adversary access beyond the Ivanti device. All information in CSAT was encrypted using AES 256 encryption and information from each application had additional security controls limiting the likelihood of lateral access. Encryption keys were hidden from the type of access the threat actor had to the system.

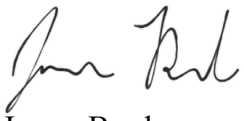
Recommendations for Impacted Individuals

While the investigation found no evidence of credentials being stolen, we would advise you to read and follow CISA's guidance on how to protect yourself from Brute Force Attacks Conducted by Cyber Actors (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), Choosing and Protecting Passwords (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), and Multi-Factor Authentication (https://www.cisa.gov/MFA).

[3] For more on this type of malicious activity, visit: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

CISA has created a website with copies of this notice, frequently asked questions, periodic updates, and an opportunity to sign up for an email distribution list to receive updates on the website. As CISA explores additional possible remediations, we encourage you to sign up to our distribution list for this incident to receive all the latest updates at www.cisa.gov/csat-notification. Questions about this incident by impacted individuals should be addressed to the CISA Chemical Security Subdivision at CFATS.Notifications@cisa.dhs.gov.

Sincerely,



James Burd
Chief Privacy Officer

Sprechen Sie kein Englisch? Bitte besuchen Sie www.cisa.gov/csat-notification und wählen Sie Ihre bevorzugte Sprache für diesen Brief.

Sprechen Sie kein Englisch? Bitte besuchen Sie www.cisa.gov/csat-notification und wählen Sie Ihre bevorzugte Sprache für diesen Brief.

انگلیسی صحبت نمی کنید؟ لطفاً از www.cisa.gov/csat-notification دیدن کنید و زبان مورد نظر خود را برای این نامه انتخاب کنید.

Vous ne parlez pas anglais ? Veuillez visiter www.cisa.gov/csat-notification et choisir votre langue préférée pour cette lettre.

अंग्रेज़ी नहीं बोलते हैं? कृपया www.cisa.gov/csat-notification पर जाएँ और इस पत्र के लिए अपनी पसंदीदा भाषा को चुनें।

英語以外の言語で本通知を確認する場合は、www.cisa.gov/csat-notification をより、希望の言語を選択してください。

영어를 사용하지 않습니까? www.cisa.gov/csat-notification 을 방문하여 이 편지에 대해 원하는 언어를 선택하세요.

Hindi nakakapagsalita ng Ingles? Mangyaring bumisita sa www.cisa.gov/csat-notification at piliin ang mas gusto mong wika para sa liham na ito.

不懂英语？请访问 www.cisa.gov/csat-notification ， 选择您喜欢的语言来阅读这封信。

不懂英語？請訪問 www.cisa.gov/csat-notification 選擇您喜歡的語言來閱讀這封信。