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

皆様

ご存知のとおり、サイバーセキュリティ・インフラストラクチャー・セキュリティー庁 (CISA) の化学物質セキュリティー評価ツール (CSAT) は、2024 年 1 月 23 日から 2024 年 1 月 26 日にかけて悪意のある攻撃者によるサイバーセキュリティー侵入の標的となり、その結果、化学テロリズム脆弱性情報（CVI）の認定ユーザーの人員保証プログラムへの提出情報およびアカウントに不正アクセスされる可能性がありました。

CISAの調査では、このデータが流出した証拠は見つかりませんでしたが、個人情報（PII）をCISAの化学施設テロ対策基準（CFATS）プログラムに提出し審査を受けていた、またはCVI認定ユーザー・アカウントを持っていたすべての方々に対し、この情報が不適切にアクセスされた可能性があることをお知らせします。今回の侵入未遂に関して、私たちが知り得る情報を皆様に提供します。

本通知をお受け取りになっているのは、（１）制限区域のある、および/または重要資産のある化学施設側で、人員保証プログラムの審査のために、皆様の個人情報を提出した可能性があるため、もしくは（２）ご自身または化学施設側で、2007年6月から2023年7月の間に、CVI Authorized Userアカウントを作成するために、限定的な個人情報および業務連絡先情報を入力した過去があるため、のどちらかが理由になります。また、今回の不正アクセス未遂に関し、皆様と関係のある化学施設にも技術的な詳細を共有しました。

影響を受けた可能性のある情報について

人員保証プログラムCFATS人員保証プログラムは、CFATS規制対象施設が、リスク・ベース・パフォーマンス基準（RBPS）12（iv）-に準拠することを可能にしました。RBPS 12(iv) [1]は、高リスク化学施設の立ち入り禁止エリアや重要資産へのアクセスを持っている、またはアクセスしようとしていた施設職員および付き添いのない訪問者に対し、テロとのつながりの可能性がないか検査することを義務付けました。これには、CSATを通じて個人情報を提出し、直接審査を行ったり、テロリスト照会用データベース[2]と照合するために、国土安全保障省の他のプログラムで実施された審査を再利用したりすることが含まれます。

[1] 6 C.F.R. 27.230(a)(12(iv).
[2]テロリスト照会データベースについてのさらなる情報は、以下を確認してください。https://www.fbi.gov/investigate/terrorism/tsc

人員保証プログラムを通じて提出された個人情報には、個人の氏名、生年月日、市民権、性別が含まれていました。米国籍以外の方には、必要に応じてさらに以下のような個人情報が提出されていました。

- 別名
- 出生地
- 国籍
- パスポート番号
- 受付番号
- 番号
- グローバルエントリー番号
- TWIC ID番号

*CSATユーザーアカウント*一般に、CSATに情報を提出する施設には、2種類のユーザー・アカウントがあります： トップスクリーン調査、セキュリティ脆弱性評価、およびサイト・セキュリティ計画の提出または策定に関与するCSATユーザー（CVI認定ユーザーを含む）、および人員保証情報を提出するCSATユーザーです。いずれの場合も、CSATアカウント作成のために収集される情報は同じです：氏名、役職、勤務先住所、勤務先電話番号。

不正アクセスの詳細

1 月 26 日、CISA は、CSAT Ivanti Connect Secure アプライアンスに影響を与える悪意の[3]可能性があるアクセスを確認しました。CISA はただちにシステムをオフラインにし、アプリケーションをネットワークの残りの部分から隔離し、フォレンジック調査を開始しました。この調査には、CISA の最高情報責任者室、サイバーセキュリティ部門の脅威ハンティング チーム、国土安全保障省のネットワーク オペレーション センターの技術専門家が参加しました。

調査中、本アクセス実行者が Ivanti デバイスに高度なウェブシェルをインストールしていたことを特定しました。このタイプの Web シェルは、悪意のあるコマンドを実行したり、基盤となるシステムにファイルを書き込んだりするために使用される場合があります。さらなる分析により、悪意のある攻撃者が 2 日間にわたって Web シェルに数回アクセスしたことが特定されました。

重要なこととして、本調査は終了し、CSATからのデータの流出や、Ivantiデバイス以外へのアクセスは確認されていません。CSATの情報はすべてAES256で暗号化され、各アプリケーションからの情報はさらにセキュリティ管理され、外部からのアクセ

[3]この様なタイプの悪意あるアクセスの詳細については、https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b をご覧ください。

スの可能性を制限していました。暗号化キーは、今回の脅威者がシステムにアクセスするタイプから隠されていました。

影響を受けた可能性のある皆様へ

今回 の調査では、認証情報が盗まれた証拠は見つかりませんでしたが、サイバー行為者による総当たり攻撃（https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors）、パスワードの選択と保護（https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords）、多要素認証（https://www.cisa.gov/MFA）から身を守る方法に関するCISAのガイダンスを読み、遵守されることをお勧めします。

CISAは本件に関わるウェブサイトを開設し、本ウェブサイト内で、本通知の掲載、よくある質問、定期的な更新情報及びメーリングリストに登録するページを作成しました。CISAは、引き続き本件の調査を続けていきますので、本件に関わる最新情報を取得されたい場合は、www.cisa.gov/csat-notification よりメールリストへの登録をしてください。本件の影響を受けた疑いがある方でご質問のある方は、CISA 化学セキュリティ部門 (CFATS.Notifications@cisa.dhs.gov) までご連絡ください。

敬具

ジェームズ・バード
個人情報保護管理者