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

Le 20 juin 2024

Cher collègue,

Comme vous le savez peut-être, l'outil d'évaluation de la sécurité chimique (CSAT), de l'Agence pour la Cybersécurité et la Sécurité des Infrastructures (CISA) a été la cible d'une intrusion, par un acteur malveillant du 23 janvier 2024 au 26 janvier 2024, ce qui a entraîné un accès non autorisé potentiel aux soumissions du programme de garantie du personnel et des comptes des utilisateurs qui ont accès, aux Informations sur la Vulnérabilité Chimique-Terroriste (CVI).

Bien que l'enquête de la CISA n'ait trouvé aucune preuve d'exfiltration de ces données, nous informons toutes les personnes dont les informations personnelles identifiables (PII) ont été soumises Normes Antiterroristes des Installations Chimiques de la CISA (CFATS), pour vérification, ou qui possèdent un compte d'utilisateur autorisé de l'IVE, par excès de prudence, que ces informations pourraient avoir été consultées de manière inappropriée. Je partage votre inquiétude et votre frustration, et je vous communique les informations dont nous disposons sur cette tentative d'intrusion.

Vous recevez cette notification parce que, (1) une installation chimique où vous aviez, des zones à accès restreint et/ou à des actifs critiques peut avoir soumis des IIP vous concernant, pour vérification dans le cadre du programme de garantie du personnel, ou (2) vous ou une installation chimique avez soumis des IIP limitées et des coordonnées professionnelles pour la création d'un compte d'utilisateur autorisé de l'IVE entre les dates de juin 2007 et de juillet 2023. Nous avons également contacté l'installation chimique à laquelle vous êtes associé pour obtenir des détails techniques sur l'intrusion.

Informations Potentiellement Concernées

Programme de Garantie du Personnel. Le Programme de Garantie du Personnel du CFATS a permis aux installations réglementées par le CFATS de se conformer à la Norme de Performance Basée sur le Risque (RBPS) 12(iv) - Garantie du Personnel. L'article 12(iv) des RBPS[1] exigeait que le personnel de l'installation et les visiteurs non accompagnés qui avaient, ou cherchaient à avoir accès à des zones d'accès restreint, et à des biens essentiels dans des installations chimiques à haut risque, fassent l'objet d'un contrôle afin de détecter d'éventuels liens avec des terroristes. Il s'agissait notamment, de soumettre des IPI par l'intermédiaire du CSAT en vue d'un contrôle direct, ou de réaffecter des contrôles effectués dans le cadre d'autres programmes du Ministère de la Sécurité Intérieure afin de comparer les personnes, à la Base de Données de Contrôle des Terroristes[2].

[1] 6 C.F.R. 27.230(a)(12(iv).
[2] Pour en savoir plus sur la base de données de dépistage du terrorisme, consultez le site : https://www.fbi.gov/investigate/terrorism/tsc

Les IIP soumises dans le cadre du programme de cautionnement du personnel comprenaient le nom, la date de naissance, la nationalité ou le sexe d'une personne. Des IIP supplémentaires ont été fournies, si celles-ci sont disponibles, ou requises pour une personne non américaine, notamment :

. Alias
. Lieu de Naissance
. Citoyenneté
. Numéro de Passeport
. Numéro de Secours
. Un Numéro
. Numéro d'Identification de l'Entrée Global
. Numéro ID TWIC

Comptes d'utilisateurs CSAT. En général, il existe deux types de comptes d'utilisateur pour les installations qui soumettent des informations au CSAT : Les utilisateurs du CSAT qui soumettent ou participent à l'élaboration des enquêtes Top-Screen, des évaluations des vulnérabilités en matière de sécurité et des plans de sécurité des sites (y compris les utilisateurs autorisés de l'IVE), et les utilisateurs du CSAT qui soumettent des informations relatives à la garantie du personnel. Dans les deux cas, les informations collectées pour la création d'un compte CSAT sont les mêmes : nom, titre, adresse professionnelle et numéro de téléphone professionnel.

Détails de l'intrusion

Le 26 janvier, CISA a identifié une activité potentiellement malveillante[3] affectant l'appliance Ivanti Connect Secure du CSAT. Le CISA a immédiatement mis le système hors ligne, isolé l'application du reste du réseau et entamé une enquête médico-légale. Cette enquête a été menée par des experts techniques du bureau du directeur de l'information de la CISA, de l'équipe de chasse aux menaces de notre division de cybersécurité et du centre d'opérations du réseau du ministère de la sécurité intérieure.

Au cours de l'enquête, nous avons identifié qu'un acteur malveillant avait installé un système web avancé sur l'appareil Ivanti. Ce type de service peut être utilisé pour exécuter des commandes malveillantes, ou écrire des fichiers sur le système sous-jacent. Notre analyse a également révélé qu'un acteur malveillant a accédé au webshell (ce système web) à plusieurs reprises au cours d'une période de deux jours.

Il est important de noter que l'enquête est terminée, et qu'elle n'a pas permis d'identifier d'exfiltration de données du CSAT, ou d'accès d'adversaires au-delà de l'appareil Ivanti. Toutes les informations contenues dans le CSAT ont été cryptées, à l'aide du cryptage AES 256 et les informations provenant de chaque application ont fait l'objet de contrôles de sécurité

[3] Pour en savoir plus sur ce type d'activité malveillante, consultez le site : https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

supplémentaires limitant la probabilité d'un accès latéral. Les clés de chiffrement étaient cachées, par rapport au type d'accès au système dont disposait l'auteur de la menace.

Recommandations pour la personne touchée

Bien que l'enquête n'ait révélé aucune preuve de vol d'informations d'identification, nous vous conseillons de lire et de suivre les conseils de la CISA sur la manière de vous protéger contre les Attaques par Force Brute Menées par des Cyber Acteurs (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), le choix et la protection des mots de passe (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), et l'authentification multifactorielle (https://www.cisa.gov/MFA)..

La CISA a créé un site web contenant des copies de cet avis, des questions fréquemment posées, des mises à jour périodiques et la possibilité de s'inscrire sur une liste de distribution par courrier électronique afin de recevoir les mises à jour du site web. Alors que la CISA étudie d'autres solutions possibles, nous vous encourageons à vous inscrire sur notre liste de distribution concernant cet incident, afin de recevoir toutes les dernières mises à jour à l'adresse www.cisa.gov/csat-notification. Les questions des personnes concernées sur cet incident doivent être adressées à la Sous-Division de la sécurité Chimique de la CISA à l'adresse suivante : CFATS.Notificiations@cisa.dhs.gov.

Sincèrement,

James Burd
Responsable de la confidentialité