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

Juni 20, 2024

Sehr geehrte Kolleginnen und Kollegen,

Wie Sie vielleicht wissen, war das Chemical Security Assessment Tool (CSAT) der Cybersecurity and Infrastructure Security Agency (CISA) vom 23. Januar 2024 bis zum 26. Januar 2024 Ziel eines Cyberangriffs durch einen bösartigen Akteur, was zu einem potenziell unbefugten Zugriff auf Einsendungen des Personnel Surety Program und Konten für Autorisierte Benutzer von Chemical-terrorism Vulnerability Information (CVI) führte.

Obwohl die Untersuchung der CISA keine Hinweise auf eine Exfiltration dieser Daten ergab, benachrichtigen wir alle Personen, deren personenbezogene Daten (PII) im Rahmen des Chemical Facility Anti-Terrorism Standards (CFATS) Programms der CISA zur Überprüfung eingereicht wurden oder die ein CVI-Autorisierter Benutzerkonto hatten, aus Vorsicht, dass diese Informationen möglicherweise unangemessen abgerufen wurden. Ich teile Ihre Besorgnis und Frustration und stelle Ihnen die Informationen zur Verfügung, die wir über diesen versuchten Einbruch wissen.

Sie erhalten diese Benachrichtigung, weil (1) eine Chemieanlage, zu der Sie Zugang zu eingeschränkten Bereichen und/oder kritischen Vermögenswerten hatten, möglicherweise PII von Ihnen zur Überprüfung im Rahmen des Personnel Surety Program eingereicht hat, oder (2) Sie oder eine Chemieanlage zwischen Juni 2007 und Juli 2023 begrenzte PII und Geschäftskontaktdaten für die Erstellung eines CVI-Autorisierten Benutzerkontos eingereicht haben. Wir haben auch die Chemieanlage, mit der Sie verbunden sind, bezüglich technischer Details des Einbruchs kontaktiert.

Möglicherweise Betroffene Informationen

Personnel Surety Program. Das CFATS Personnel Surety Program ermöglichte es CFATS-regulierten Anlagen, den Risk-Based Performance Standard (RBPS) 12(iv) —Personnel Surety einzuhalten. RBPS 12(iv)[1] erforderte, dass Anlagenpersonal und unbegleitete Besucherinnen, die Zugang zu eingeschränkten Bereichen und kritischen Vermögenswerten in hochriskanten Chemieanlagen hatten oder suchten, auf mögliche terroristische Verbindungen überprüft wurden. Dies beinhaltete das Einreichen von PII über CSAT zur direkten Überprüfung oder die Wiederverwendung von Überprüfungen, die im Rahmen anderer Programme des Department of Homeland Security durchgeführt wurden, um Einzelpersonen gegen die Terrorist Screening Database[2] zu überprüfen.

[1] 6 C.F.R. 27.230(a)(12)(iv).
[2] Weitere Informationen zur Terrorist Screening Database finden Sie unter: https://www.fbi.gov/investigate/terrorism/tsc

Über das Personnel Surety Program eingereichte PII umfasste den Namen, das Geburtsdatum, die Staatsangehörigkeit oder das Geschlecht einer Person. Zusätzliche PII wurde bereitgestellt, sofern verfügbar oder für eine nicht-US-Person erforderlich, einschließlich:

- Aliase
- Geburtsort
- Staatsangehörigkeit
- Reisepassnummer
- Abhilfe-Nummer
- A-Nummer
- Global Entry ID-Nummer
- TWIC ID-Nummer

CSAT-Benutzerkonten. Im Allgemeinen gibt es zwei Arten von Benutzerkonten für Einrichtungen, die Informationen für CSAT einreichen: CSAT-Benutzer, die Top-Screen-Umfragen, Sicherheitslückenbewertungen und Standort-Sicherheitspläne einreichen oder daran beteiligt sind (einschließlich CVI-autorisierter Benutzer) und CSAT-Benutzer, die Personal-Sicherheit-Informationen einreichen. In beiden Fällen sind die Informationen, die für die Erstellung eines CSAT-Kontos gesammelt werden, dieselben: Name, Titel, Geschäftsadresse und Geschäftstelefonnummer.

Details des Einbruchs

Am 26. Januar identifizierte CISA potenziell bösartige Aktivitäten[3], die CSAT Ivanti Connect Secure Appliance betrafen. CISA nahm das System sofort offline, isolierte die Anwendung vom Rest des Netzwerks und begann eine forensische Untersuchung. Diese Untersuchung umfasste technische Experten aus dem Büro des Chief Information Officer der CISA, dem Threat Hunting Team unserer Cybersecurity Division und dem Network Operations Center des Department of Homeland Security.

Während der Untersuchung identifizierten wir, dass ein bösartiger Akteur eine fortschrittliche Webshell auf dem Ivanti-Gerät installiert hatte. Diese Art von Webshell kann verwendet werden, um bösartige Befehle auszuführen oder Dateien auf das zugrunde liegende System zu schreiben. Unsere Analyse ergab weiter, dass ein bösartiger Akteur die Webshell mehrmals über einen Zeitraum von zwei Tagen aufgerufen hat.

Wichtig ist, dass die Untersuchung abgeschlossen ist und keine Datenexfiltration von CSAT oder ein gegnerischer Zugriff über das Ivanti-Gerät hinaus identifiziert wurde. Alle Informationen in CSAT wurden mit AES-256-Verschlüsselung verschlüsselt und Informationen aus jeder Anwendung hatten zusätzliche Sicherheitskontrollen, die die Wahrscheinlichkeit eines seitlichen Zugriffs begrenzten. Verschlüsselungsschlüssel waren vor der Art des Zugriffs, den der Bedrohungsakteur auf das System hatte, verborgen.

[3] Weitere Informationen zu dieser Art von bösartigen Aktivitäten finden Sie unter: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

Empfehlungen für Betroffene

Obwohl die Untersuchung keine Hinweise auf gestohlene Anmeldeinformationen ergab, raten wir Ihnen, die CISA-Richtlinien zu lesen und zu befolgen, wie Sie sich vor Brute-Force-Angriffen durch Cyberakteure schützen können (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), Passwörter auswählen und schützen (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords) und Multi-Faktor-Authentifizierung (https://www.cisa.gov/MFA).

CISA hat eine Website erstellt, auf der Kopien dieser Mitteilung, häufig gestellte Fragen, regelmäßige Updates und die Möglichkeit zur Anmeldung für eine E-Mail-Verteilerliste zum Erhalt von Updates auf der Website verfügbar sind. Da CISA zusätzliche mögliche Abhilfemaßnahmen untersucht, empfehlen wir Ihnen, sich in unsere Verteilerliste für diesen Vorfall einzutragen, um die neuesten Updates unter www.cisa.gov/csat-notification zu erhalten. Fragen zu diesem Vorfall von betroffenen Personen sollten an die CISA Chemical Security Subdivision unter CFATS.Notificiations@cisa.dhs.gov gerichtet werden.

Mit freundlichen Grüßen,

James Burd
Chief Privacy Officer