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

20 जून, 2024

प्रिय सहकर्मी,

हो सकता है कि आप जानते हों, साइबर सुरक्षा और अवसंरचना सुरक्षा एजेंसी (CISA) का रासायनिक सुरक्षा मूल्यांकन उपकरण (CSAT) 23 जनवरी, 2024 से 26 जनवरी, 2024 के बीच किसी दुर्भावनापूर्ण कर्ता द्वारा साइबर सुरक्षा में की गई अतिक्रमण के प्रति लक्षित हुआ था, जिसके परिणामस्वरूप कार्मिक प्रतिभूति कार्यक्रम प्रस्तुतियाँ और रासायनिक-आतंकवाद अतिसंवेदनशील जानकारी (CVI) के अधिकृत उपयोगकर्ताओं के खातों तक संभावित अनधिकृत पहुंच की गई थी।

जबकि CISA की जांच-पड़ताल में इस डेटा के चोरी होने का कोई सबूत नहीं मिला है, फिर भी हम अत्यधिक सावधानी के तहत उन सभी व्यक्तियों को सूचित कर रहे हैं, जिन्होंने अपनी व्यक्तिगत पहचान योग्य जानकारी (PII) CISA के रसायनिक सुविधा-स्थल के आतंकवाद-विरोधी मानकों (CFATS) के प्रोग्राम में जांच के लिए प्रस्तुत की थी या जिनके पास CVI अधिकृत उपयोगकर्ता खाता था, कि इस जानकारी तक अनुचित तरीके से पहुंच की गई हो सकती है। मैं आपकी चिंता और निराशा को समझ सकता हूँ तथा अतिक्रमण के इस प्रयास के बारे में हमें जो जानकारी पता है, उससे आपको अवगत करवा रहा हूँ।

आपको यह सूचना इसलिए मिल रही है क्योंकि (1) एक रासायनिक सुविधा-स्थल, जहाँ आपको प्रतिबंधित क्षेत्रों और/या महत्वपूर्ण परिसंपत्तियों तक पहुंच थी, ने कार्मिक प्रतिभूति प्रोग्राम के तहत जांच के लिए आपकी PII प्रस्तुत की हो सकती है या (2) आपने या किसी रासायनिक सुविधा-स्थल ने जून 2007 और जुलाई 2023 के बीच CVI अधिकृत उपयोगकर्ता खाते के निर्माण के लिए सीमित PII और व्यावसायिक संपर्क जानकारी प्रस्तुत की हो सकती है। हमने इस अतिक्रमण के बारे में तकनीकी विवरण के लिए उस रासायनिक सुविधा-स्थल से भी संपर्क किया है जिससे आप संबंधित हैं।

संभावित रूप से प्रभावित जानकारी

कार्मिक प्रतिभूति कार्यक्रम। CFATS कार्मिक प्रतिभूति कार्यक्रम ने CFATS द्वारा विनियमित सुविधा-स्थलों को जोखिम-आधारित प्रदर्शन मानक (RBPS) 12(iv) — कार्मिक प्रतिभूति का अनुपालन करने में सक्षम बनाया है। RBPS 12(iv)[1] के अनुसार उच्च जोखिम वाले रासायनिक संयंत्रों में प्रतिबंधित क्षेत्रों और महत्वपूर्ण परिसंपत्तियों तक पहुंच बनाने वाले या पहुंच करने वाले संयंत्र कर्मियों और अकेले आगंतुकों की संभावित आतंकवादी संबंधों के लिए जांच की जानी आवश्यक है। इसमें प्रत्यक्ष जांच के लिए CSAT के ज़रिए PII प्रस्तुत करना या आतंकवादी स्क्रीनिंग डेटाबेस में व्यक्तियों की जांच करने के लिए होमलैंड सुरक्षा विभाग के अन्य कार्यक्रमों के तहत की गई जांच को पुन: अभिप्रेत करना शामिल था।[2]

---

[1] 6 C.F.R. 27.230(a)(12(iv).
[2] आतंकवादी स्क्रीनिंग डेटाबेस के बारे में अधिक जानकारी के लिए, यहाँ जाएँ: https://www.fbi.gov/investigate/terrorism/tsc

कार्मिक प्रतिभूति कार्यक्रम के ज़रिए सबमिट की गई PII में किसी व्यक्ति का नाम, जन्म तिथि, नागरिकता, या लिंग शामिल था। अगर उपलब्ध थी या किसी गैर-अमेरिकी व्यक्ति के लिए ज़रूरी थी, तो अतिरिक्त PII प्रदान की गई थी, जिसमें शामिल है:

- अन्य नाम
- जन्म का स्थान
- नागरिकता
- पासपोर्ट नम्बर
- निवारण नम्बर
- A नम्बर
- ग्लोबल एंट्री आईडी नम्बर
- TWIC आईडी नम्बर

CSAT उपयोगकर्ता खाते. सामान्य रूप से, CSAT के लिए जानकारी प्रस्तुत करने वाले सुविधा-स्थलों के लिए दो प्रकार के उपयोगकर्ता खाते होते हैं: शीर्ष-स्क्रीन सर्वेक्षण, सुरक्षा अतिसंवेदनशीलता आकलन, और साइट सुरक्षा योजनाओं (CVI अधिकृत उपयोगकर्ताओं को शामिल करने के लिए) को विकसित करने में शामिल या कार्मिक प्रतिभूति जानकारी प्रस्तुत करने वाले CSAT उपयोगकर्ता। दोनों ही मामलों में, CSAT खाता बनाने के लिए इकट्ठी की गई जानकारी एक जैसी होती है: नाम, पद, व्यवसाय का पता और व्यवसाय का फ़ोन नंबर।

अतिक्रमण का विवरण

26 जनवरी को, CISA ने CSAT Ivanti Connect Secure उपकरण को प्रभावित करने वाली संभावित दुर्भावनापूर्ण गतिविधि[3] की पहचान की। CISA ने तुरंत ही सिस्टम को ऑफलाइन कर दिया, ऐप्लिकेशन को मुख्य नेटवर्क से अलग कर दिया, तथा फोरेंसिक जांच-पड़ताल शुरू कर दी। इस जांच-पड़ताल CISA का मुख्य सूचना अधिकारी कार्यालय, हमारे साइबर सुरक्षा प्रभाग की थ्रेट हंटिंग टीम और होमलैंड सुरक्षा विभाग के नेटवर्क ऑपरेशन सेंटर के तकनीकी विशेषज्ञ शामिल थे।

इस जांच-पड़ताल के दौरान, हमने पाया कि किसी दुर्भावनापूर्ण व्यक्ति ने Ivanti उपकरण पर एक उन्नत वेबशेल इंस्टॉल किया था। इस प्रकार के वेबशेल का इस्तेमाल दुर्भावनापूर्ण कमांड्स को निष्पादित करने या अंतर्निहित सिस्टम में फ़ाइलें लिखने के लिए किया जा सकता है। हमारे विश्लेषण से आगे यह भी पता चला कि किसी दुर्भावनापूर्ण कर्ता ने दो दिन की अवधि में कई बार इस वेबशेल तक पहुंच की थी।

महत्वपूर्ण बात यह है कि जांच-पड़ताल पूरी हो चुकी है और इसमें CSAT से डेटा की चोरी या Ivanti डिवाइस से परे दुश्मन द्वारा पहुंच किये जाने का पता नहीं चला है। CSAT में सारी जानकारी AES 256 एन्क्रिप्शन का इस्तेमाल करके एन्क्रिप्ट की गई थी और प्रत्येक ऐप्लिकेशन से जानकारी में अतिरिक्त सुरक्षा नियंत्रण मौजूद थे, जिससे पार्श्व पहुंच किए जाने की संभावना सीमित हो गई थी। एन्क्रिप्शन कुंजियों को दुर्भावनापूर्ण कर्ता की सिस्टम तक की पहुंच से छिपाया गया था।

[3] इस प्रकार की दुर्भावनापूर्ण गतिविधि के बारे में अधिक जानकारी के लिए, यहाँ जाएँ: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

प्रभावित हुए व्यक्तियों केलिए सिफ़ारिशें

हालाकि जांच में क्रेडेंशियल्सचोरी होने का कोई सबूत नहीं मिला है, फिर भी हम आपको सलाह देंगेकि साइबर कर्ताओं द्वारा किए जाने वाले Brute Force अटैक से खुद को बचाने के लिए CISA के दिशा-निर्देशों(https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), पासवर्डों का चयन करना औए उन्हें सुरक्षित रखना (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), और बहु-कारक प्रमाणीकरण (https://www.cisa.gov/MFA) को पढ़ें और उनका पालन करें।

CISA ने इस नोटिस की प्रतियाँ, अक्सर पूछेजाने वाले प्रश्न, आवधिक अपडेट्स और वेबसाइट पर अपडेट्स प्राप्त करने केलिए ईमेल वितरण सूची केलिए साइन अप करने का मौका प्रदान करते हुए एक वेबसाइट बनाई है। जबकि CISA अतिरिक्त संभावित समाधानों की खोज कर रहा है, हम आपको इस घटना के लिए हमारी वितरण सूची में साइन अप करने के लिए प्रोत्साहित करते हैं ताकि आप www.cisa.gov/csat-notification पर सभी नवीनतम अपडेट्स प्राप्त कर सकें। प्रभावित व्यक्तियों को इस घटना केबारे में अपने परश्न CISA रासायनिक सुरक्षा उप-विभाग से CFATS.Notifications@cisa.dhs.gov केज़रिए पूछने चाहिए।

आपका शुभचिंतक,

James Burd
मुख्य गोपनीयता अधिकारी