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

Hunyo 20, 2024

Mahal na Katrabaho,

Gaya ng maaaring nalalaman mo na, ang Tool sa Pagtatasa para sa Seguridad ng Kemikal (CSAT, ang akronima nito sa Ingles) ng Ahensya ng Cybersecurity at Seguridad na Pang-imprastruktura (CISA, ang akronima nito sa Ingles) ay pinuntirya ng panlulusob sa cybersecurity ng isang mapaminsalang kasangkapan mula Enero 23, 2024 hanggang Enero 26, 2024, na nagresulta sa potensyal na hindi awtorisadong pag-access sa mga pagsusumite at account ng Programa ng Seguridad ng mga Tauhan (Personnel Surety Program) para sa mga Awtorisadong Gumagamit ng Impormasyon sa Pagkabulnerable sa Terorismong Kemikal (CVI, ang akronima nito sa Ingles).

Habang walang natagpuan ang imbestigasyon ng paglilipat ng data na ito, inaabisuhan namin ang lahat ng indibidwal na nagsumite ng kanilang personal na matutukoy na impormasyon (PII, ang akronima nito sa Ingles) sa programa ng Mga Pamantayan ng Pasilidad ng Kemikal Laban sa Terorismo (CFATS, ang akronima nito sa Ingles) para sa pagsisiyasat o nagkaroon ng account para sa Awtorisadong Gumagamit ng CVI mula sa dami ng pag-iingat na ang impormasyong ito ay maaaring na-access sa hindi naaangkop na paraan. Nakikiisa ako sa iyong pag-aalala at pagkayamot at nagbibigay ako sa iyo ng impormasyong nalalaman namin hinggil sa tinangkang panlulusob na ito.

Natanggap mo ang paunawang ito dahil (1) isang kemikal na pasilidad kung saan may access ka sa mga pinaghihigpitang lugar at/o mga kritikal na asset ang maaaring nakapagsumite ng PII tungkol sa iyo para sa pagsisiyasat sa ilalim ng Programa ng Seguridad ng mga Tauhan o (2) ikaw o isang kemikal na pasilidad ay nagsumite ng may limitasyong PII at impormasyong pangnegosyo sa pakikipag-ugnayan para sa paglikha ng account para sa Awtorisadong Gumagamit ng CVI sa pagitan ng mga petsa ng Hunyo 2007 at Hulyo 2023. Nakipag-ugnayan din kami sa kemikal na pasilidad na ikaw ay nauugnay hinggil sa mga teknikal na detalye tungkol sa panlulusob.

Impormasyon na Posibleng Naapektuhan

Programa ng Seguridad ng mga Tauhan. Ang Programa ng Seguridad ng mga Tauhan ng CFATS ay nagbigay-daan para sa mga pasilidad na pinangangasiwaan ng CFATS na sumunod sa Pamantayan ng Pagganap na Nakabatay sa Panganib (RBPS, ang akronima nito sa Ingles) 12(iv) —Seguridad ng mga Tauhan. Inatasan ng RBPS 12(iv)[1] ang mga tauhan ng pasilidad at mga hindi sinasamahang bisita na nagkaroon o humihiling ng access sa mga mga pinaghihigpitang lugar at mga kritikal na access sa mga pasilidad ng kemikal na may mataas na panganib na masiyasat para sa mga posibleng kaugnayan sa terorista. Kabilang dito ang pagsusumite ng PII

[1] 6 C.F.R. 27.230(a)(12(iv).

sa pamamagitan ng CSAT para sa direktang pagsisiyasat o iniaakmang pagsisiyasat na isinasagawa sa ilalim ng iba pang mga programa ng Kagawaran ng Seguridad ng Bansa (Department of Homeland Security) upang masiyasat ang mga indibidwal sa Database sa Pagsisiyasat ng Terorista (Terrorist Screening Database)[2].

Kabilang sa PII na isinumite sa pamamagitan ng Programa ng Seguridad ng mga Tauhan ang pangalan, petsa ng kapanganakan, pagkamamamayan, o kasarian ng indibidwal. Nagbigay ng karagdagang PII, kung mayroon man o kailangan para sa indibidwal na hindi taga-U.S., kabilang ang:

- Mga Alyas
- Lugar ng Kapanganakan
- Pagkamamamayan
- Numero ng Pasaporte
- Numero ng Redress
- Numero sa Green Card (A Number)
- Numero ng Global Entry ID
- Numero ng TWIC ID

Mga Account ng Gumagamit sa CSAT. Sa pangkalahatan, may dalawang uri ng mga account ng gumagamit para sa mga pasilidad na nagsusumite ng impormasyon para sa CSAT: ang mga gumagamit ng CSAT o nakikibahagi sa pagbuo ng mga Top-Screen survey, Mga Pagtatasa sa Pagkabulnerable ng Seguridad, at mga Plano ng Seguridad ng Lugar (upang isama ang mga awtorisadong gumagamit ng CVI) at mga gumagamit ng CSAT na nagsusumite ng impormasyon sa seguridad ng mga tauhan. Sa magkatulad na kaso, ang impormasyong nakolekta para sa paggawa ng CSAT account ay pareho: pangalan, titulo, address ng negosyo, at numero ng telepono ng negosyo.

Mga Detalye ng Panlulusob

Noong Enero 26, tinukoy ng CISA ang posibleng mapaminsalang aktibidad[3] na nakakaapekto sa CSAT Ivanti Connect Secure na kasangkapan. Agad na kinuha ng CISA ang system offline, ibinukod ang aplikasyon sa buong network, at sinimulan ang porensik na imbestigasyon. Kasama sa imbestigasyong ito ang mga teknikal na eksperto mula sa Tanggapan ng Punong Opisyal ng Impormasyon ng CISA, pangkat ng Tumitingin ng Panganib (Threat Hunting team) ng Dibisyon ng Cybersecurity, at ng Sentro ng mga Operasyon ng Network ng Kagawaran ng Seguridad ng Bansa.

Sa imbestigasyong ito, tinukoy namin ang mapaminsalang kasangkapan na nailagay sa pinakabagong webshell sa device na Ivanti. Ang ganitong uri ng webshell ay maaaring magamit upang maglabas ng mga mapaminsalang command o sumulat ng mga file sa nakapaloob na

[2] Para sa higit pang impormasyon tungkol sa Database sa Pagsisiyasat ng Terorista, bumisita sa: https://www.fbi.gov/investigate/terrorism/tsc

[3] Para sa higit pang impormasyon tungkol sa ganitong uri ng mapaminsalang aktibidad, bumisita sa: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

system. Higit pang tinukoy sa aming pagsusuri na ang mapaminsalang kasangkapan ay na-access ang webshell nang maraming beses sa loob ng dalawang araw.

Mahalaga pa, nagtapos ang imbestigasyon at hindi natukoy ang paglipat ng data mula sa CSAT o hindi tamang pag-access nang higit pa sa device ng Ivanti. Ang lahat ng impormasyon sa CSAT ay naka-encrypt gamit ang AES 256 encryption at ang impormasyon mula sa bawat aplikasyon ay nagkaroon ng mga karagdagang kontrol na panseguridad na naglilimita sa posibilidad ng kaugnay na pag-access. Nakatago ang mga encryption key sa uri ng pag-access na mayroon ang nagbabantang kasangkapan sa system.

Mga Rekomendasyon para sa mga Naapektuhang Indibidwal

Habang walang natagpuan ang imbestigasyon ng patunay ng pagnanakaw ng mga kredensyal, papayuhan ka naming basahin at sundin ang gabay ng CISA tungkol sa kung paano mapoprotektahan ang iyong sarili mula sa Mararahas na Puwersa ng Pag-atake na Isinasagawa ng mga Pumipinsala sa Cyber (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), Pagpili at Pagprotekta sa mga Password (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords), at Multi-Factor na Authentication (https://www.cisa.gov/MFA).

Gumawa ang CISA ng website na may mga kopya ng paunawang ito, mga madalas itanong, mga pana-panahong update, at isang oportunidad para mag-sign up para sa listahan ng padadalhan ng email para makatanggap ng mga update tungkol sa website. Habang tinutuklas ng CISA ang mga karagdagang posibleng remedyasyon, hinihikayat ka naming mag-sign up sa aming listahan ng padadalhan ng email para sa insidenteng ito upang matanggap ang lahat ng pinakabagong update sa www.cisa.gov/csat-notification. Ang mga katanungan tungkol sa insidenteng ito ng mga naapektuhang indibidwal ay dapat maiparating sa Subdibisyon sa Seguridad sa Kemikal (Chemical Segurity Subdivision) ng CISA sa CFATS.Notificiations@cisa.dhs.gov.

Taos-puso,

James Burd
Punong Opisyal sa Pagkapribado