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

20 de junio de 2024

Estimado colega:

Como bien sabe, la Herramienta de Evaluación de Seguridad Química (CSAT, por sus siglas en inglés) de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) fue objeto de una intrusión de ciberseguridad por parte de un actor malintencionado entre el 23 de enero de 2024 y el 26 de enero de 2024. Esto dio lugar a un posible acceso no autorizado a comunicaciones del Programa de Garantía del Personal (Personnel Surety Program) y a cuentas de usuarios autorizados para el acceso a información sobre vulnerabilidad ante el terrorismo químico (CVI, por sus siglas en inglés).

Si bien la investigación de Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) no encontró pruebas de la filtración de estos datos, estamos notificando a todas las personas que presentaron su información de identificación personal (PII, por sus siglas en inglés) ante el programa Estándares Antiterroristas de Instalaciones Químicas (CFATS, por sus siglas en inglés) de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) con fines de investigación o que tenían una cuenta de usuario autorizado para el acceso a información sobre vulnerabilidad ante el terrorismo químico (CVI). Lo hacemos por precaución, teniendo en cuenta que alguien pudo haber accedido a esta información de manera inapropiada. Comparto su preocupación y su frustración, y le facilito la información que tenemos sobre este intento de intrusión.

Está recibiendo esta notificación porque (1) una instalación química en la que usted tenía acceso a zonas restringidas o a activos críticos puede haber presentado su información de identificación personal (PII) para que sea investigada en el marco del Programa de Garantía del Personal, o bien porque (2) usted o una instalación química presentaron dicha PII limitada y su información de contacto comercial con el propósito de crear una cuenta de usuario autorizado para el acceso a información sobre vulnerabilidad ante el terrorismo químico (CVI) entre las fechas de junio de 2007 y julio de 2023. También nos hemos puesto en contacto con la instalación química con la que usted está asociado en relación con los detalles técnicos de la intrusión.

Información que puede verse afectada

Programa de Garantía del Personal. El Programa de Garantía del Personal, que pertenece al programa Estándares Antiterroristas de Instalaciones Químicas (CFATS), permitió que las instalaciones reguladas por el CFATS cumplan con la parte IV de la norma 12, Garantía de Personal, de las Normas de Desempeño Basadas en el Riesgo (RBPS, por sus siglas en inglés). En dicha regulación, se exigía que el personal de las instalaciones y los visitantes sin escolta que tuvieran o pretendieran tener acceso a zonas restringidas y a activos críticos en

instalaciones químicas de alto riesgo[1] fueran sometidos a un control para detectar posibles vínculos terroristas. Esto incluía la presentación de información de identificación personal (PII) a través de Herramienta de Evaluación de Seguridad Química (CSAT) para la investigación directa o la reutilización de la investigación realizada en el marco de otros programas del Departamento de Seguridad Nacional (Department of Homeland Security) con el fin de cotejar a las personas con la base de datos de detección de terroristas.[2]

La información de identificación personal (PII) presentada a través del Programa de Garantía del Personal incluía el nombre, la fecha de nacimiento, la nacionalidad o el sexo de una persona. Se proporcionó información de identificación personal (PII) adicional, si estaba disponible o si era necesaria para una persona no estadounidense, lo que incluyó lo siguiente:

- Seudónimos
- Lugar de nacimiento
- Ciudadanía
- Número de pasaporte
- Número de compensación
- Un número
- Número de identificación de Global Entry
- Número de identificación de TWIC

Cuentas de usuario de la Herramienta de Evaluación de Seguridad Química (CSAT). En general, existen dos tipos de cuentas de usuario para las instalaciones que envían información a la Herramienta de Evaluación de Seguridad Química (CSAT): los usuarios de esta herramienta que envían o participan en el desarrollo de encuestas de la aplicación Top-Screen, de las Evaluaciones de Vulnerabilidad de la Seguridad (Security Vulnerability Assessments) y de los Planes de Seguridad del Sitio (Site Security Plans) (lo que incluye a a los usuarios autorizados para el acceso a información sobre vulnerabilidad ante el terrorismo químico [CVI]), y los usuarios de esta herramienta que envían información de garantía del personal. En ambos casos, la información recopilada para la creación de una cuenta de la Herramienta de Evaluación de Seguridad Química (CSAT) es la misma: nombre, cargo, dirección profesional y número de teléfono profesional.

Detalles de la intrusión

El 26 de enero, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) identificó una actividad potencialmente[3] maliciosa que afectaba a la aplicación Ivanti Connect Secure de la Herramienta de Evaluación de Seguridad Química (CSAT). La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) desconectó inmediatamente el sistema, aisló la aplicación del resto de la red e inició una investigación forense. Esta investigación incluyó a expertos técnicos de la Oficina del Director de Información (Office of the Chief

[1] 6 C.F.R. 27.230(a)(12(iv).
[2] Para obtener más información sobre la base de datos de detección de terroristas, visite: https://www.fbi.gov/investigate/terrorism/tsc
[3] Para obtener más información sobre este tipo de actividad maliciosa, visite https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b

Information Officer) de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA), el equipo de Caza de Amenazas (Threat Hunting) de nuestra División de Ciberseguridad (Cybersecurity Division) y el Centro de Operaciones de Red del Departamento de Seguridad Nacional (Department of Homeland Security's Network Operations Center).

Durante la investigación, identificamos que un actor malicioso instaló un shell web avanzado en el dispositivo Ivanti. Este tipo de shell web puede utilizarse para ejecutar comandos maliciosos o escribir archivos en el sistema subyacente. Nuestro análisis identificó, además, que un actor malicioso accedió a la shell web varias veces durante un periodo de dos días.

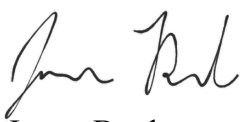
Es importante destacar que la investigación ya concluyó y que no se ha identificado ninguna filtración de datos de la Herramienta de Evaluación de Seguridad Química (CSAT) ni ningún acceso de adversarios, más allá de lo ocurrido con el dispositivo Ivanti. Toda la información de la Herramienta de Evaluación de Seguridad Química (CSAT) se encriptó utilizando el cifrado AES 256, y la información de cada aplicación tenía controles de seguridad adicionales que limitaban la probabilidad de acceso lateral. Las claves de cifrado se ocultaban para impedir el tipo de acceso al sistema que tenía el actor de la amenaza.

Recomendaciones para los afectados

Aunque la investigación no encontró pruebas de robo de credenciales, le aconsejamos que lea y siga las directrices de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) sobre cómo protegerse de los ataques de fuerza bruta llevados a cabo por ciberactores (https://www.cisa.gov/news-events/alerts/2018/03/27/brute-force-attacks-conducted-cyber-actors), sobre la elección y la protección de contraseñas (https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords) y sobre la autenticación multifactor (https://www.cisa.gov/MFA).

La Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) ha creado un sitio web con copias de este aviso, con preguntas frecuentes, con actualizaciones periódicas y con la oportunidad de inscribirse en una lista de distribución de correo electrónico para recibir las novedades del sitio web. Mientras la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) explora posibles soluciones adicionales, lo invitamos a suscribirse a nuestra lista de distribución relacionada con este incidente para recibir las últimas novedades en www.cisa.gov/csat-notification. Las preguntas de las personas afectadas sobre este incidente deben dirigirse a la Subdivisión de Seguridad Química (Chemical Security Subdivision) de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA) en CFATS.Notifications@cisa.dhs.gov.

Atentamente,



James Burd
Director de Protección de Datos