La Oficina del Auditor del Estado de Washington (SAO), dijo el lunes que está investigando un incidente de seguridad que resultó en el compromiso de la información personal de más de 1.6 millones de personas que presentaron reclamos de desempleo en el estado en 2020.

La SAO culpó de la violación a una vulnerabilidad de software en el servicio File Transfer Appliance (FTA) de Accellion, que permite a las organizaciones compartir documentos confidenciales con usuarios fuera de su organización de forma segura.

> *«Durante la semana del 25 de enero de 2021, Accellion confirmó que una persona no autorizada tuvo acceso a los archivos de SAO mediante la explotación de una vulnerabilidad en el servicio de transferencia de archivos de Accellion»,* dijo la SAO en un comunicado.

La información a la que se tuvo acceso contiene detalles personales de los residentes del estado de Washington que presentaron reclamos de seguro de desempleo en 2020, así como otros datos de los gobiernos locales y agencias estatales.

La información exacta que se vio comprometida incluye:

- Nombre completo
- Número de seguridad social
- Licencia de conducir
- Número de identificación estatal
- Número de cuenta bancaria y número de ruta bancaria
- Lugar de trabajo

Al parecer, el incidente de acceso no autorizado ocurrió a fines de diciembre de 2019, aunque parece que no se conoció el alcance total de la intrusión hasta que Accellion reveló a inicios de este mes que su aplicación de transferencia de archivos era el *«objetivo de un ciberataque sofisticado»*.

La compañía de soluciones en la nube con sede en Palo Alto dijo el 11 de enero que se enteró de una vulnerabilidad en su software FTA heredado a mediados de diciembre, luego de lo cual confirmó que abordó el problema y lanzó un parche *«dentro de 72 horas»* a los más de 50 clientes afectados.

Accellion también mencionó que está contratando con una *«firma forense de ciberseguridad líder en la industria»* para investigar el incidente.

Debido a que se puede abusar de la información comprometida para llevar a cabo un robo de identidad o fraude, la SAO dijo que está en proceso de organizar medidas para proteger las identidades de aquellos cuya información puede haber estado contenida en los archivos de la SAO.

Mientras tanto, la agencia recomienda revisar los estados de cuenta y los informes de crédito, notificar a las instituciones financieras de cualquier actividad sospechosa y reportar cualquier incidente sospechoso de robo de identidad a la policía.

Cabe mencionar que el software FTA de Accellion se utilizó como vector de ataque para atacar a otras dos organizaciones, incluida la Comisión de Inversiones y Valores de Australia (ASIC) y el Banco de la Reserva de Nueva Zelanda (RBNZ) en las últimas semanas.