Caso de estudio: "EQUIFAX *data breach*" (Buró de crédito EE. UU.)

La escasa implementación de mecanismos de seguridad en el desarrollo de software permite fácilmente que un ciberdelincuente afecte directamente los pilares de la seguridad de la información, como son la confidencialidad, integridad y disponibilidad, generando pérdidas económicas importantes, además de afectar la reputación de ésta.

En septiembre del 2017, la empresa fue afectada por una brecha de seguridad importante, en la cual se filtraron 143 millones de registros que contenían información importante para validar la identidad de una persona (nombres, direcciones, teléfonos y correos electrónicos). Los costos de Equifax, vinculados al manejo de esta crisis, podrían oscilar entre los 200 y 300 millones de dólares.

¿Cómo fue comprometida?

El ataque se llevó a cabo entre los meses de marzo-junio, aprovechando que existía una falla de seguridad de Apache Struts 2, el cual es un *framework* en JAVA, un componente de tercero que no estaba actualizado en su desarrollo. Llama la atención que los desarrolladores de Struts, 2 meses antes del ataque, habían anunciado este desperfecto en su software y lanzaron una actualización de inmediato para remediar.

Referencias

Comparación de ciclos de vida de desarrollo de software seguro (S-SDLC) EQUIFAX data breach (Buro de crédito EUA), (2021). Platzi. Recuperado de https://platzi.com/tutoriales/1583-ethical-hacking/3940-comparacion-de-ciclos-de-vida-de-desarrollo-de-software-seguro-s-sdlc-2/?gclid=CjwKCAiAs8acBhA1EiwAgRFdw125mh9OilfTUh_Ni7xoghXFp56f-U_22TblNkoWHSr0Pbi2UaP1cBoCtG0QAvD_BwE&gclsrc=aw.ds