Caso Equifax

Esta lectura aborda en profundidad el caso de la brecha de Equifax en 2017, analizando su origen, desarrollo, impacto y consecuencias legales, con información verificada de fuentes oficiales y análisis independientes.

La brecha de Equifax de 2017 se inició tras la explotación de la vulnerabilidad CVE-2017-5638 en Apache Struts el 12 de mayo de 2017, permaneció oculta durante 76 días hasta su detección el 29 de julio, y comprometió datos sensibles de aproximadamente 147 millones de usuarios, incluidos números de seguridad social, fechas de nacimiento y direcciones (en.wikipedia.org, blackduck.com). La respuesta inicial fue tardía, pues a pesar de que el parche estaba disponible desde el 7 de marzo de 2017, los sistemas permanecieron expuestos y solo el 2 de agosto Equifax contrató a Mandiant para realizar una investigación forense exhaustiva (investor.equifax.com, archive.epic.org). A raíz de este incidente, Equifax enfrentó demandas agregadas y un acuerdo de hasta 700 millones de dólares con la FTC, el CFPB y 50 estados de EE. UU., además de auditorías del Senado que denunciaron negligencia en la gestión de parches y controles de seguridad insuficientes (ftc.gov, hsgac.senate.gov).

Origen y vulnerabilidad explotada

Descubrimiento de la vulnerabilidad

El 7 de marzo de 2017, Apache Software Foundation publicó un parche para la falla CVE-2017-5638 en Struts, que permitía ejecución remota de código al manipular cabeceras de contenido multipart/form-data (en.wikipedia.org). Sin embargo, Equifax no aplicó esa corrección, dejando su portal de disputas de crédito vulnerable durante más de dos meses (blackduck.com).

Explotación del sistema

El 12 de mayo de 2017, atacantes automatizaron búsquedas de instancias sin parche y consiguieron credenciales internas mediante la explotación de CVE-2017-5638 (en.wikipedia.org). Una vez dentro, ejecutaron más de 9 000 consultas cifradas a las bases de datos de crédito, extrajeron fragmentos en pequeños archivos temporales y los exfiltraron antes de eliminarlos, prolongando el acceso no detectado durante 76 días (en.wikipedia.org).

Línea de tiempo y detección

- **29 de julio de 2017**: Tras renovar un certificado SSL expirado desde hacía nueve meses, la herramienta de vigilancia de tráfico alertó sobre actividad anómala, descubriéndose el ataque (en.wikipedia.org).

- **30 de julio de 2017**: Equifax desconectó la aplicación vulnerable para contener el ataque (archive.epic.org).

- **2 de agosto de 2017**: Se contrató a la firma Mandiant para la investigación forense de la intrusión (archive.epic.org, investor.equifax.com).

- **Septiembre de 2017**: Equifax anunció públicamente la brecha tras confirmar que datos de 147 millones de personas habían sido accesados (ftc.gov).

Impacto y magnitud de los datos comprometidos

La intrusión expuso información de aproximadamente 147 millones de consumidores en EE. UU. (ftc.gov). Entre los datos filtrados estaban nombres, fechas de nacimiento, direcciones y números de seguridad social; además, en 209 000 casos se robaron números de tarjetas de crédito (vanityfair.com). El Anuario del Senado de EE. UU. reportó que el ataque afectó a 148 millones de consumidores, subrayando la magnitud del fallo de seguridad (oversight.house.gov).

Respuesta corporativa y cambios ejecutivos

En octubre de 2017, ante el escándalo, Equifax reemplazó al CEO, CIO y CSO para restaurar la confianza de inversores y público (cstl.com). Paralelamente, la compañía reforzó sus protocolos de parcheo, segmentación de red y cifrado de datos, aunque los informes del Senado señalaron que estos cambios llegaron demasiado tarde (hsgac.senate.gov).

Consecuencias legales y regulatorias

En julio de 2019, Equifax acordó pagar al menos 575 MUSD y hasta 700 MUSD como parte de un acuerdo global con la FTC, el CFPB y 50 estados de EE. UU., tras admitir falta de “pasos razonables” para asegurar sus sistemas (ftc.gov). El mismo pacto incluyó un fondo de 425 MUSD destinado a reembolsos y monitoreo de crédito para los afectados (ftc.gov). Informes del Comité de Supervisión de la Cámara concluyeron que la organización falló en gestionar un inventario de activos, priorizar vulnerabilidades críticas y adoptar controles de detección efectivos (oversight.house.gov).

Lecciones aprendidas y buenas prácticas

1. **Gestión proactiva de parches**: Adoptar ciclos automáticos que prioricen vulnerabilidades críticas inmediatamente tras su publicación (blackduck.com).

2. **Inventario de activos**: Mantener un registro exhaustivo de todos los componentes de software y hardware para asegurar cobertura de actualizaciones (en.wikipedia.org).

3. **Segmentación y cifrado**: Limitar el alcance de accesos internos y cifrar datos sensibles tanto en tránsito como en reposo (oversight.house.gov).

4. **Detección temprana**: Implementar monitoreo continuo de certificados, configuraciones y patrones de tráfico para identificar anomalías con prontitud (en.wikipedia.org).

5. **Respuesta coordinada**: Definir acuerdos de alcance claros, roles y protocolos de comunicación con terceros (e.g., Mandiant) antes de que ocurra un incidente (archive.epic.org).

En suma, la brecha de Equifax representa un caso paradigmático de los riesgos de postergar parches críticos y subestimar la complejidad de los entornos legados, recordándonos que la resiliencia cibernética exige disciplina, gobernanza rigurosa y mejora continua.