Equifax (2017) – Explotación de CVE-2017-5638 en Apache Struts

---

Resumen del incidente

Entre el 13 de mayo y el 30 de julio de 2017, atacantes aprovecharon una vulnerabilidad crítica en Apache Struts (CVE-2017-5638) para acceder sin autorización al portal de disputas de crédito de Equifax. Durante esos 76 días sustrajeron datos personales de aproximadamente 147 millones de consumidores —incluidos nombres, fechas de nacimiento, números de seguro social y licencias de conducir— antes de ser detectados tras una alerta de tráfico anómalo al renovarse un certificado SSL expirado (investor.equifax.com).

Descripción técnica de la vulnerabilidad

CVE-2017-5638 reside en el componente de subida de archivos de Struts, donde la aplicación no validaba correctamente la cabecera **Content-Type** en peticiones multipart/form-data. Al inyectar expresiones OGNL maliciosas en dicha cabecera, el atacante desencadena ejecución remota de código (RCE) en el servidor afectado sin necesidad de credenciales (revenera.com).

Evaluación del impacto

- **Volumen de datos comprometidos:** ~147 millones de registros personales en EE. UU. (investor.equifax.com).
- **Tipos de información filtrada:** nombres, SSN, fechas de nacimiento, direcciones, licencias de conducir —pone en riesgo la identidad de los usuarios—.
- **Costes legales y financieros:** Equifax acordó pagar entre 575 MUSD y 700 MUSD en multas y reparaciones a la FTC, CFPB y 50 estados de EE. UU. (ftc.gov).
- **Reputación corporativa:** pérdida de confianza masiva, investigaciones del Congreso y cambio de altos directivos.

Análisis de causas

1. **Falla en el parcheo:** a pesar de que Apache publicó la corrección el 6 de marzo de 2017, Equifax no la aplicó, incluso tras recibir una notificación del DHS al día siguiente (oversight.house.gov).

2. **Inventario de activos deficiente:** ausencia de un mapeo exhaustivo de servidores y aplicaciones que permitiera identificar y priorizar componentes vulnerables.

3. **Monitoreo insuficiente:** carencia de alertas tempranas específicas para detección de patrones OGNL maliciosos en tráfico HTTP.

Recomendaciones de seguridad

- **Gestión proactiva de parches:** implementar un flujo automatizado que aplique correcciones de alta criticidad en < 48 horas desde su publicación (oversight.house.gov).

- **Inventario dinámico de activos:** mantener un repositorio centralizado con dependencias y versiones de todas las librerías (Software Bill of Materials).

- **Segmentación de red y control de acceso:** aislar aplicaciones de frontend de bases de datos sensibles mediante zonas de confianza y firewalls internos.

- **Monitoreo y detección de anomalías:** desplegar IDS/IPS con reglas específicas para patrones OGNL y comportamientos RCE en HTTP.

- **Pruebas de penetración periódicas:** contratar ejercicios de pentesting que simulen explotación de cabeceras malformadas y validen los mecanismos de mitigación.

Conclusión ética

Un hacker ético habría identificado CVE-2017-5638 al evaluar el portal de disputas de Equifax, notificando responsablemente la incidencia antes de su explotación masiva y validando el cierre de la brecha tras parcheo. La negligencia corporativa al ignorar una alerta del DHS y retrasar el parcheo contravino principios de responsabilidad y divulgación completa propios del Código de Ética de la industria.

\Referencias

- Equifax Releases Details on Cybersecurity Incident (investor.equifax.com)
- FTC Settlement with Equifax, Inc. (ftc.gov)
- House Oversight Committee Report on Equifax Breach (oversight.house.gov)
- Revenera: Unpatched Vulnerability in Apache Struts 2 Caused Data Breach (revenera.com)