Equifax Security Breach

Joseph Pennington

Introduction

- Attackers exploited a vulnerability to exfiltrate hundreds of millions of customer records.
- The initial breach began March 10, 2017, but data was not stolen until May 13, 2017. The exact date is unknown, but it took until July 2017 for Equifax admins to identify the breach.
- The patch was applied sometime between July 2017 and September 2017 when Equifax publicized the breach.
- 143 million people's personal data was stolen. Equifax spent $1.38 billion to resolve consumer claims.

Technical Details 1

- On March 7, 2017, a known vulnerability with Apache Struts 2 was published (CVE-2017-5638).
- Apache Struts 2 is a Java framework that is used by Java-based web apps.
- This vulnerability allows attackers to include code in the “Content-Type” header of an HTTP request to be executed by a web server.

Technical Details 2

- On March 9, 2017, Equifax admins were told to apply the patch to the systems. However, the employee responsible failed to do so.
- On March 15, 2017, Equifax ran scans to identify any remining unpatched systems. The scans failed to identify the unpatched systems.
- It is not clear why the patching process failed.

Technical Details 3

- On March 10, 2017, the Equifax web portal was breached with the vulnerability.
- However, it appears that data exfiltration did not begin until May 13, 2017.
- Between May and July 2017, attackers were able to steal the data by encrypting it during exfiltration. Equifax had tools to decrypt and inspect data to spot the attack.
- However, Equifax failed to renew their public-key certificate for the inspection tool. This means encrypted traffic was not being correctly inspected.

Controls and Lessons Learned

- Effective Controls
  - Employee accountability for patching vulnerabilities quickly
  - Functioning vulnerability scanning tools
  - Effective encrypted traffic inspection software
- Lessons Learned
  - Even large companies can fall victim to a simple vulnerability exploit
  - Having separate databases provides security in depth
  - Managing access control and monitoring for anomalies is important
- Source

https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html