**Incident Report**

**Name of Reporter:** Khadijah Walker

**Name of Incident:** 2017 Equifax Breach

**Date of Incident:** March – September 2017

**Executive summary:**

In 2017, Equifax, a consumer reporting agency, discovered a data breach that exposed 143 million Americans' credit card numbers, personal identifying information, and dispute documents. Equifax's failure to update one of its certifications led to a vulnerability in Apache Struts.

**Detailed Summary:**

Before May's 2017 data breach, attackers gained access to Equifax's framework through a vulnerability in Apache Struts.

Attackers identified the vulnerability by scanning Equifax's server and discovered it was dubbed CVE-2017-5638. Usernames and passwords were in plaintext which made it easy to access additional systems. IRS, SSA, and USPS discovered there were several lower-level technical concerns and requested Equifax to address them before the breach. When attackers discovered the vulnerability in Equifax's dispute portal server, they were most likely able to send covert malicious code with an HTTP request by placing it in the content-type header. Apache Struts was tricked into executing the code, giving the attackers access to Equifax's framework. With the attacker's access, they extracted 143 million Americans' credit card numbers, personal identifying information, and dispute documents from Equifax's dispute portal. Attackers continued to exploit the website by executing 9,000 more queries of incomplete information. Data was slowly removed by attackers through encryption that looked like a daily protocol for Equifax. The data breach lasted 76 days before an irregular value was discovered through a routine scan of Apache Struts. Equifax began remediating the issue by patching affected systems on March 9, 2017, and the investigation continued.

Once patches and signatures were updated, several signs of intrusion were detectable. It was believed that the attacker was an amateur but Equifax's personal information was not being sold on the dark web which concluded that that was not accurate. So, through further research, Equifax discovered similarities to espionage attacks, executed by the Chinese. Equifax charged the four Chinese military members for the 2017 Equifax data breach. Equifax continued to make remediations by reconstructing its sequence installation and removing certain knowledge-based questions from its verification questions. Equifax gave consumers a website, <https://www.equifaxsecurity2017.com>, to check if personal information was stolen during the 2017 data breach. The website consisted of a discrepancy that led consumers to the wrong website and gave them a reply of a "positive breach," even if consumers had not been breached. If consumers lost funds due to the breach, Equifax gave each affected consumer $125. Ultimately, victims of the Equifax data breach benefited from the $425 million settlement. Equifax is also a source for many major federal customers; IRS, SSA, USPS, oversight companies; BCFS, CRA, and FTC. Equifax did a press release on September 7, 2017, notifying consumers of the breach without notifying their federal customers. BCFS requested immediate information about the breach and then released a blog on the top 10 ways consumers could protect themselves. IRS, SAA, and USPS checked to see if their consumers were affected by cross-referencing Equifax's list of breached consumers. IRS and SSA changed their contracts to require updates within one hour of an indicator of compromise.

**Major Findings:**

* When Equifax scanned their servers through active scanning, there were no vulnerabilities detected
* Equifax scanned servers after signatures were updated and all the vulnerabilities that attackers found were visible
* Between March to May of 2017, Equifax was a victim of a data breach.
* Apache Struts contained expired signatures.
* Used an open-source platform with critical vulnerabilities.
* Equifax asked too many knowledge-based questions.
* Equifax believed the Chinese were able to extract information through espionage.
* Declined services from DHS

**Recommendations for Remediation:**

* Equifax consults with DHS as they are responsible for protecting and preventing cyber incidents.
* Firewall segmentation for each sector of personal information
* Install IDS/IPS firewall.
* Hire a designated network security engineer to patch servers.
* Host leadership briefings on the significance of signatures and accuracy.

**Conclusion:**

The 2017 Equifax breach was one of the largest data breaches ever, affecting over 143 million Americans. The espionage data breach of Apache Struts can be used as a reference to help prevent future breaches. Prioritizing and protecting a company’s assets is the primary lesson used by today’s cybersecurity teams.