Equifax Data Breach: Cybersecurity Analysis Report

1. Introduction:

In one of the most significant data breaches of the 21st century, Equifax, one of the three major credit reporting agencies in the United States, suffered a catastrophic cyberattack in mid-2017. The breach compromised the personal information of approximately 147 million individuals, including names, social security numbers, birth dates, addresses, and in some cases, driver's license numbers. This case study explores how the breach occurred, the vulnerabilities exploited, the compromised components of the CIA triad, the attackers' tactics, techniques, and procedures (TTPs), and the post-breach mitigation efforts taken by Equifax.

2. CIA Triad Compromise:

The CIA triad—Confidentiality, Integrity, and Availability—is a foundational model for cybersecurity. In the case of the Equifax breach:

- **Confidentiality** was **severely compromised**. Sensitive personal data of millions was accessed and exfiltrated by unauthorized actors.
- **Integrity** was potentially at risk but no confirmed manipulation of data was reported.
- **Availability** was not directly affected in this attack; Equifax systems remained operational during and after the breach.

Thus, the primary compromise was to **confidentiality**, which had long-term implications for personal privacy and identity theft risks.

3. TTPs (Tactics, Techniques, and Procedures):

The attackers used a combination of known tactics to exploit Equifax's systems:

- **Tactic**: Exploitation of a known vulnerability.
- **Technique**: Remote Code Execution via **Apache Struts vulnerability** (CVE-2017-5638).

- **Procedure**: After identifying the unpatched system, attackers sent crafted HTTP requests that triggered the vulnerability, allowing them to execute arbitrary commands on Equifax's web application server.

Once inside, the attackers:

- Established **persistence**.
- Conducted **lateral movement** within the network.
- Accessed and exfiltrated sensitive data undetected for **76 days**.

4. Vulnerability Exploited:

The core vulnerability that enabled this breach was **Apache Struts CVE-2017-5638**, a remote code execution flaw in the Jakarta Multipart parser used in the Apache Struts framework. Despite the fact that a patch was released on **March 7, 2017**, Equifax **failed to patch** the vulnerability in a timely manner.

This oversight allowed the attackers to send specially crafted HTTP requests containing malicious content-types, resulting in remote execution of commands on Equifax's web servers. The attack began on **May 13, 2017**, over two months after the patch was available.

5. Motive Behind the Attack:

Although the attackers were never officially identified, U.S. federal prosecutors later charged four members of the **Chinese military** (People's Liberation Army) with the attack. The motive appeared to be **nation-state cyber-espionage** rather than financial gain. The stolen data—particularly Social Security numbers, full names, birth dates, and addresses—could be used for long-term intelligence purposes, including identity theft, blackmail, and tracking of U.S. citizens.

6. Detection and Mitigation:

The breach was discovered on **July 29, 2017**, when suspicious network traffic was noticed. Equifax took the affected web application offline, conducted an internal investigation, and disclosed the breach publicly on **September 7, 2017**.

Key mitigation steps included:

- Patching the Apache Struts vulnerability.
- Engaging a cybersecurity firm (Mandiant) to assess and remediate the breach.
- Setting up consumer credit monitoring services.
- Improving internal security processes including:
    - Asset management
    - Patch management
    - Network segmentation
    - Intrusion detection and response

7. Lessons Learned:

This breach highlighted several critical cybersecurity failures:

1. **Lack of timely patching**: Despite knowing the vulnerability existed, Equifax failed to act quickly.
2. **Poor asset inventory and scanning**: The vulnerable system was not identified during internal scans.
3. **Inadequate monitoring**: The breach went undetected for over two months.
4. **Weak internal communication and accountability** in handling vulnerabilities.

Organizations must prioritize **vulnerability management**, **incident response readiness**, and **proactive monitoring** to prevent such breaches.

8. Conclusion:

The Equifax data breach serves as a stark reminder of how a single unpatched vulnerability can lead to a massive compromise of personal data. It emphasizes the need for robust cybersecurity practices, especially in organizations that handle sensitive consumer information. The breach not only affected millions of individuals but also caused significant reputational and financial damage to Equifax, with settlements costing the company over $700 million. Strengthening the principles of the CIA triad and implementing rigorous TTP detection mechanisms is essential in preventing such incidents in the future.