**Research Report**

|  |  |
| --- | --- |
|  | **Topic**  Equifax Data Breach (2017)  **Prepared By** Tayyaba Asif  **Date**  6 Aug 2025 |

Contents

[Equifax Data Breach (2017) 2](#_Toc205320938)

[Introduction 2](#_Toc205320939)

[Overview of Incident How Did it occur? 2](#_Toc205320940)

[What Information Leaked? 2](#_Toc205320941)

[Reason of the Attack 3](#_Toc205320942)

[In What Way was the Vulnerability used? (TTPs) 3](#_Toc205320943)

[Impact on CIA Triad 3](#_Toc205320944)

[Equifax Consequences 3](#_Toc205320945)

[Lessons Learned 4](#_Toc205320946)

[Conclusion 4](#_Toc205320947)

[References 4](#_Toc205320948)

# Equifax Data Breach (2017)

## Introduction

In our modern world, cybercrime has become a highly significant issue, and the example of the Equifax data breach in 2017 is widely provided as an excellent example of how just one vulnerability can lead to massive complications [1]. Equifax is among the three biggest companies in the United States that generate credit reports by gathering financial data of people. The company failed to upgrade its software on the company website promptly; therefore, hackers were able to gain access to the personal details of the company, which were very sensitive personal information of nearly 147 million individuals [2]. Many cybersecurity professionals were shocked by this event, because it was so preventable- it occurred because of irresponsibility, not a high-level cybersecurity hacking technique.

## Overview of Incident How Did it occur?

It occurred between the middle of May and July 2017, yet it was not publicly revealed until September 2017 [3]. The hackers exploited a security bug in one of the web software called Apache Struts, which Equifax deployed in its online dispute system. This vulnerability (CVE-2017-5638) enabled remote code execution vulnerability, that is, the attackers only needed to send specially crafted web requests to make the server execute their own malicious commands [3]. Although Equifax had been aware of this problem, and a security update had been already issued in March 2017, the company failed to apply the patch in time [4]. Because of this delay, the cybercriminals gained lots of time to access the system, navigate the system, and steal much data away.

## What Information Leaked?

The stolen information contained the full names, dates of birth, Social Security Numbers (SSNs), home addresses, telephone numbers, driver licence details, approximately 209000 credit card numbers and personal dispute documents of approximately 182000 customers [2]. Such type of information is highly sensitive as it can be utilized by criminals to hijack identity, open unauthorized bank accounts, borrow money or commit other forms of financial related crimes.

## Reason of the Attack

According to experts, the primary motive of the attack was financial [5]. The dark web also pays big money because your personal identity data, and in particular, the Social Security Number (SSN) can be used by criminals over several years. Identity numbers are normally permanent as compared to the passwords which individuals can simply change. This makes them to be of great interest to the hackers who seek to earn some cash by selling the information to others or engaging in one way or the other financial frauds.

## In What Way was the Vulnerability used? (TTPs)

These hackers followed a number of steps in their hacking campaign commonly referred to as Tactics, Techniques & Procedures (TTPs). To begin with, they found a way into the system by exploiting a vulnerability on one of the web applications that was publicly available. Then they applied a type of remote code execution, which is sending malicious orders via HTTP header, to have the server execute their malicious program [3]. Once they were inside, they remained in the system and penetrated further into the network since there were no corresponding internal barriers. They did not want to get caught because Equifax lacked effective monitoring. Lastly, they gradually and cautiously transferred the stolen data out of the system of Equifax to their personal computers [4].

## Impact on CIA Triad

The confidentiality was deeply affected, with personal information of millions of people being exposed [2]. Nothing was compromised in terms of Integrity since the data was not altered nor impaired by the attackers and since Equifax systems had been functioning normally Availability was not compromised either [1].

## Equifax Consequences

This was a cost or damage to Equifax in terms of reputation and consequent financial costs. Very soon after the incident, all the CEO, CIO, and CSO of the company resigned [1]. Equifax was sued by many governments and consumers. In 2019 Equifax reached an agreement to pay not less than 575 million dollars (potentially up to 700 million dollars) to the U.S. Federal Trade Commission [2]. Along with the monetary fines, Equifax had to lose the trust of its customers, not mentioning its value as the long-term example of convenience at the expense of cybersecurity.

## Lessons Learned

The Equifax hack shows how useful straightforward cybersecurity controls such as maintaining software current, running great monitoring, and network dividing the network properly- are. Businesses must ensure all their systems are updated, they should periodically test weak points, educate employees on the issue of cybersecurity, and promptly respond in the event that a threat is detected. This breech would have been prevented very easily by Equifax, had they made use of the security patches on Apache Struts, as they came into the company.

## Conclusion

The hack of Equifax is discussed as one of the most vital cybersecurity incidents over the last several years. It reveals that even a slightest disregard of some software update may cause a huge number of people with their personal data being revealed. This hack was detrimental to the Confidentiality of the CIA triad. It was financially driven and took advantage of an existing bug of a web application. Generally, we learn that cybersecurity is not associated with high-tech only, it is about responsibility and taking simple precautions in time.

## References

1.Equifax. (2017). 2017 Cybersecurity Incident & Important Consumer Information.

2. U.S. Government Accountability Office (2018). Report on the Equifax Data Breach.

3. CVE MITRE. (2017). CVE-2017-5638 (Apache Struts 2 vulnerability).

4. Krebs, B. (2017). How Hackers Broke In: Unpatched Vulnerability in Apache Struts. KrebsOnSecurity.

5. Smith, J. (2019). The Equifax Data Breach: Analysis of Causes and Impact. Journal of Cybersecurity, 5(2), 45–52.