The Equifax Data Breach

Alexander Kotzian
Old Dominion University
CYSE 300: Introduction to Cybersecurity
Professor Malik A. Gladden
September 8, 2024

The Equifax Data Breach

In 2017 one of the most impactful cybersecurity breaches in recent memory occurred. This breach had widespread effects impacting millions of individuals and numerous businesses. The entity that was breached in this cyberattack was Equifax, which is a credit reporting agency. The information this company holds is incredibly confidential and exposes the privacy of individuals it had records of reporting on. This imposes a major concern regarding the company's cybersecurity practices as it has due responsibility to uphold the safety of that information. Therefore I aim to answer the following; What were the cybersecurity vulnerabilities? What exploited the vulnerabilities? What were the repercussions of the breach? What cybersecurity measures could have been taken to mitigate the consequences or prevent the breach.

The Equifax breach was caused by a series of events that culminated into a vulnerability being exposed. The primary issue was caused by a recently detected vulnerability found in Apache Struts software, which had been announced along with a security update by the developer. However, the lack of action taken by the responsible equifax employee in the allotted time caused the vulnerability to stay apparent in the software unnoticed. (Smith, 2017) (Glenn, 2018)

The official statement by Apache Struts regarding the vulnerability exploited was that they suspected the specific vulnerability was potentially a nine year old zero-day-exploit on CVE-2017-9805 that had been unpatched by Equifax after patches to combat the exploit had been announced. (Gielen, 2017) This exploit was the direct cause of the Equifax breach which was infiltrated by a hacker or a group of hackers who identified this vulnerability and proceeded to exploit it.

This cybersecurity breach had a multitude of repercussions associated with it. Millions of Americans' private social information was exposed to these hackers. As for the suspected hackers, in 2020 indictment charges were brought against “Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei” by the U.S. Department of Justice with a trial still pending for the suspected perpetrators of the breach. (FBI, 2020) Additionally Equifax and the Federal Trade Commission reached a settlement that forced Equifax to relinquish $425 million towards those affected by the data breach. (FTC, 2024)

This breach could have been easily avoided if Equifax had redundancies put in place in the event of something like this happening. Increased effort in vulnerability screening and additional security layers would have prevented this attack. Failing to abide by an audit they had in 2015, Equifax did not implement recommended superior patching techniques or automated patching tools, this would have provided a redundancy that would have alerted the company to the vulnerability. (115th Congress, 2018).

In conclusion, the Equifax breach was a notable cybersecurity failure within our recent past. The reliance on a single employee to implement an update once notified that there was a vulnerability within CVE-2017-9805 of Apache Struts proved detrimental to the users of Equifax. This vulnerability was exploited to victimize millions of Americans. People suffered their right to privacy, the suspects are being charged, and Equifax is forced to spend $425 million to make the victims whole. Equifax could have easily prevented this with the guidance insinuated by the audit performed in 2015, in addition to simple redundancies. Although more data breaches similar to this will occur, I hope corporations, governments, and individuals can learn how to protect themselves from privacy breaches similar to the Equifax breach.

References

Smith, R. (2017). Prepared Testimony of Richard F. Smith before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection. https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf

Glenn, Ashton, "Equifax: Anatomy of a Security Breach" (2018). Honors College Theses. 378. https://digitalcommons.georgiasouthern.edu/honors-theses/378

Gielen, R. (2017, September 9). *Apache struts statement on Equifax Security Breach*. The Apache Software Foundation Blog. https://news.apache.org/foundation/entry/apache-struts-statement-on-equifax

FBI. (2020, February 10). *Chinese hackers charged in Equifax Breach*. https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

FTC. (2024, July 24). *Equifax Data Breach Settlement*. Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement#:~:text=The%20company%20has%20agreed%20to,affected%20by%20the%20data%20breach.

Committee on Oversight and Government Reform, The Equifax Data Breach: Majority Staff Report, 115th Congress (2018). Washington, D.C. https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf