The Equifax Data Breach was one of the most significant security breaches in recent history. It happened in 2017 and exposed the sensitive personal information of 147 million U.S. citizens and 15 million British citizens. The stolen data included Social Security numbers, birth dates, addresses, driver’s licenses, and even credit card information. The reason this case made headlines is that Equifax is a credit reporting agency that people trust to protect their financial data. The attack was completely preventable, as hackers exploited an unpatched vulnerability in Equifax’s web application, something that should have been fixed long before the breach occurred.

The attack was a cyber intrusion that took advantage of a known vulnerability in Apache Struts, a framework Equifax used for its dispute resolution portal. Hackers gained access to the system and were able to move freely, stealing data over several months before the breach was even detected. Because Equifax stores massive amounts of personally identifiable information (PII), they were an obvious target for cybercriminals looking to commit identity theft and financial fraud. The immediate threat was that attackers had access to highly sensitive personal data, which could be used for fraud, identity theft, or sold on the dark web. The long-term risk was even worse: if Equifax didn’t resolve the issue, attackers could continue stealing more records, manipulating credit scores, or even compromising other financial institutions. Additionally, public trust in Equifax and other credit agencies took a major hit, as people realized their personal data wasn’t as safe as they thought.

A developer could have easily prevented this breach by ensuring that software patches were applied as soon as they became available. The Apache Struts vulnerability had been public knowledge for months, and a patch had been released, but Equifax failed to install it. Other key security measures that could have helped include real-time monitoring for unusual activity, proper network segmentation to limit access, and regular security audits to catch vulnerabilities before they could be exploited.

To stop similar breaches in the future, companies should enforce stricter security policies, such as a Patch Management Policy to ensure that known security vulnerabilities are fixed immediately, an Intrusion Detection and Prevention Policy to use automated monitoring tools to detect and respond to suspicious behavior in real time, and a Data Encryption Policy to encrypt sensitive data both in transit and at rest so that even if an attacker gets in, the data remains protected.

One of the biggest takeaways from this case is that companies must follow best security practices like using Authentication, Authorization, and Accounting (Triple A) along with Defense in Depth strategies. Multi-factor authentication (MFA) could have added an extra layer of protection against unauthorized access. Role-based access control (RBAC) would have restricted access to sensitive data, reducing the risk of internal threats. Additionally, log monitoring and security audits could have helped detect the breach much sooner. Defense in Depth (layering security controls like firewalls, intrusion detection systems, endpoint security, and network segmentation) would have made it much harder for attackers to move through Equifax’s system.

The Equifax breach is a perfect example of how poor security practices can lead to massive consequences. If Equifax had followed basic security best practices, such as timely patching, monitoring, and layered defenses, they could have avoided this entire disaster. The breach serves as a warning that companies handling sensitive data must take cybersecurity seriously, because once that trust is broken, it’s hard to earn back.