Incident Report

Name of Reporter: Leonard Sterling
Name of Incident: Equifax Breach
Date of Incident: March 2017

Executive summary:
The company Equifax had a breach that affected 143 million customers. This breach started back in march 2017. The company Equifax had to spend 1.38 billion to resolve customer claims against the company.

Detailed Summary:
The Equifax data breach was a major cyber attack that occurred in 2017 and affected 147 million people. The hackers accessed a wide range of personal information, including names, and social security numbers. Over 209,000 people had their credit card numbers stolen. This breach was a result of a vulnerability in Equifax's web application software the company failed to patch in a timely manner.The vulnerability was apache struts a framework for creating web applications written in java. The consequences of the breach were significant for both Equifax and for the individuals affected. The breach had huge affect on Equifax stock price dropped following the announcement of the breach. The company faced numerous investigations and lawsuits. Affected individuals faced a high risk of identity theft and fraud advised to take steps to protect themselves such as placing a freeze on their credit. Equifax had implemented a number of changes to its cybersecurity practices and procedures. It also reached a settlement with the Federal Trade Commission which required the company to pay up to $700 million in fines and compensation to affected individuals. The data breach was a reminder of the importance of cybersecurity and the need for companies to take appropriate measures to protect their customers personal information. It also highlighted the potential consequences of failing to do so including financial and reputational damage.The nation state threat actor that were charged was the chinese military.

Major Findings:

- A web application wasn’t patched in a timely manner
- It was multiple vulnerabilities once Equifax IT did a scan
- CVE 24 February 2021
  https://nvd.nist.gov/vuln/detail/cve-2017-5638

- On March 7th 2017 a critical vulnerability in the apache struts software was publicly disclosed.

Recommendations for Remediation:

- Run more scans on the network to ensure customers/company data is secure
- Make sure applications have the latest updates
- Make sure SOC is up to date on the latest vulnerabilities
-

Conclusion:

It was briefly mentioned how the breach happened but didn’t really describe what techniques were used to gain access to the web application. This could help other companies on what not to do and avoid a breach of this magnitude.