Equifax Data Breach (2017):

Exploitation of
Unpatched Vulnerabilities

Equifax:

Credit Reporting and
Financial Services

Affected Parties:

- 147 Million Americans
- Individuals in UK and Canada

Attack Category:

Exploitation of Unpatched Vulnerabilities - Apache Struts Vulnerability (CVE-2017-5638)

Exploitation of Unpatched Vulnerabilities - Apache Struts Vulnerability (CVE-2017-5638)

Method

- Targets known security flaws in software, systems, or applications that have not been updated with the latest security patches.
- Attackers exploit these known vulnerabilities to:
  - Gain unauthorized access.
  - Inject malicious code.
  - Cause system failures.

Statistic

- According to the 2023 IBM X-Force Threat Intelligence Index:
  - 34% of breaches in 2022 were attributed to exploiting known but unpatched vulnerabilities.

Equifax Data Breach (2017)

Overview:

Company Description

&

Breach Summary

Equifax Description:

Industry:

- Financial Services, Credit Reporting

About:

- One of the top three credit reporting agencies in the U.S., managing data for over 800 million consumers
- Provides credit reports, credit scores, and identity verification services.

Breach Summary:

Date:

- Discovered July 2017, disclosed September 2017

Attack Vector:

- Exploitation of an unpatched Apache Struts vulnerability (CVE-2017-5638) allowing remote code execution.

Impact:

- Data compromised for 147 million individuals, including names, Social Security numbers, birth dates, addresses, and credit card details.

Key Failures:

- Delayed patching of a known vulnerability.
- Breach went undetected for over two months.

Aftermath:

- Widespread legal action, regulatory fines, and significant reputational damage.
- Considered one of the largest and most damaging breaches due to the sensitivity of the data exposed.

Timeline

1 **March 7, 2017:**
Apache Struts vulnerability (CVE-2017-5638) is publicly disclosed and a patch is released.

2 **March 10, 2017:**
Equifax’s IT department was informed about the patch but failed to apply it.

3 **May 13, 2017:**
Attackers begin exploiting the unpatched vulnerability to access Equifax’s systems.

4 **July 29, 2017:**
Equifax detects suspicious network traffic indicating a potential breach.

5 **August 2, 2017:**
Equifax confirms that sensitive data was stolen.

6 **September 7, 2017:**
Equifax publicly discloses the breach.

Vulnerabilities

The Equifax breach occurred due to the exploitation of a known but unpatched vulnerability in the Apache Struts framework (CVE-2017-5638). The company failed to apply a security patch that had been available for months, allowing attackers to infiltrate their systems and exfiltrate sensitive data. Weaknesses in Equifax's network segmentation, incident response, and monitoring capabilities worsened the impact of the breach.

Failure to Patch Known Vulnerability

Despite being notified about the Apache Struts flaw, Equifax did not apply the patch, leaving systems exposed to attack.

Inadequate Network Segmentation

Poor separation between critical systems allowed attackers to move laterally and access sensitive data once inside the network.

Weak Monitoring and Detection

Went undetected for over two months, indicating insufficient network monitoring and delayed threat detection.

Poor Incident Response Planning

Breach was slow, resulting in delayed public disclosure and mishandling of the aftermath, further compounding the damage.

Costs to Equifax

&

Prevention Methods

Costs

Financial Penalties:

- Over $1.4 billion in settlements, fines, and legal fees.
- Includes a $700 million settlement with the FTC, CFPB, and U.S. states.

Operational Losses:

- Significant expenses in strengthening IT infrastructure and cybersecurity measures.
- Long-term monitoring costs for affected customers.

Reputation Damage:

- Loss of consumer trust and credibility.
- Stock value drop and ongoing reputational harm.

Prevention

Patch Management:

- Implement automated systems to ensure timely updates and security patches.

Enhanced Monitoring and Detection:

- Deploy continuous threat monitoring and early detection tools to identify suspicious activity.

Improved Incident Response:

- Regularly update and test incident response plans, including clear communication protocols for swift action during breaches.