DATA BREACH CASE STUDY

EQUIFAX
(2017)

REMOTE CODE EXECUTION (RCE)

Remote Code Execution (RCE) is an injection attack that targets leverage arbitrary code execution (ACE) vulnerabilities, which can exist virtually anywhere.

An ACE vulnerability is a security flaw commonly brought about through poor memory handling practices, allowing users of a service to inject code into the instruction pointer of a running process.

While it's not always a critical issue on its own, when successful RCE attacks are chained with privilege escalation, the attackers can potentially compromise any resource on a given server or network.

Unfortunately, these vulnerabilities are becoming more and more common. In 2019, 28.1% of all common vulnerabilities were injection-based, and 67% of those were types of RCE vulnerabilities – ranging from local or remote file inclusion to unsanitized file uploads.

EQUIFAX

Equifax, one of the three biggest consumer credit reporting agencies, found itself victim to one of the most impactful data breaches of this century, and serves as a testament to the fact that every company needs an adequate Cybersecurity team.

On September 8, 2017, Equifax released a public announcement that it had fallen victim to a cyberattack, resulting in a data breach. Shockingly, the personal data of 148 million US citizens were compromised, including legal names, birth dates, SSN numbers, and driver's license information. Along with the personal data leaked, approximately 209,000 credit card numbers were also leaked.

This situation was aggravated further when, during cleanup, customer service representatives directed victims to a phishing site via their Twitter feed, which resulted in more victims of identity theft.

- March 3 - Apache Struts CVE-2017-5638 discovered, enabling RCE attacks via exception handling issues in the Jakarta Multipart parser, which is used when a user uploads files.
- March 7 - Apache Software Foundation releases patch for CVE-2017-5638.
- March 8 - Department of Homeland Security notifies Equifax and other credit agencies of the vulnerability and patch, advising all affected parties to patch as soon as possible.
- March 9 - Apache Software Foundation directs Equifax System Admins to install the patch.
- March 15 - Equifax conducts vulnerability scan, which did not show a vulnerability to CVE-2017-5638. The Equifax IT team decides against patching Apache Struts.
- July 29 – Equifax investigates suspicious internal network activity, resulting in an announcement of the compromise of over 146 million individuals' private data.

HOW IT HAPPENED

Timeline of events leading up to the 2017 Equifax Data Breach

VULNERABILITIES

Overview

- To gain a foothold into the Equifax network, Apache Struts was exploited to gain a web shell from a parser used when users upload files.
- Though initial point of compromise was Apache Struts, it is clear to see that the IT systems management and overall security infrastructure at Equifax was inadequate.

Specific Vulnerabilities

- CVE-2017-5638
  - ACE/RCE through a web shell was the first indicator of compromise
- IT Systems Management issues
  - Negligence on the part of Equifax's IT team allowed for the initial pivot point in this attack
- Poor Cybersecurity Compliance Framework
  - To obtain the private data in this integrity breach, the attackers had to escalate their privileges, which indicates poor access control, and noncompliance with ISO 27001
- Out Of Date Network Security tools
  - The Equifax IT team stated that their vulnerability scanners reported no vulnerabilities, which indicates that their tools are/were severely out of date, which may lead to vulnerabilities and, eventually, compromise.

COST VS PREVENTION ANALYSIS

Costs

- Equifax lost $600 million in a settlement in 2019
- Equifax stock (EFX) went down $31.1 per share
- Equifax lost many customers, as well as the trust of their other customers

Prevention

- Always apply patches of critical or important severity as soon as possible, roll out other patches weekly or monthly.
- Their Cybersecurity Compliance Framework shouldn't have allowed for negligence or out-of-date vulnerability assessment tools.
- Proper configuration and update management of IDS and SIEM tools should have been implemented to reliably detect incidents within the network.
- Equifax should have implemented an ISMS following ISO 27001 to allow for more in-depth access control compliance.

REFERENCES

- https://www.imperva.com/blog/the-state-of-vulnerabilities-in-2019/
- https://www.digitalshadows.com/blog-and-research/an-update-on-the-equifax-data-breach/
- https://vixra.org/pdf/1808.0215v1.pdf