WhiteSource

Your Equifax Brief: Understanding the Key Facts and Lessons Learned

Who is Equifax?

One of the Big Three credit rating agencies in the US, Equifax collects and aggregates financial and personal data of over 800M individual consumers, as well as some 80M businesses. Equifax offers credit information to businesses and credit monitoring & fraud prevention services to consumers.

EQUIFAX

What is Apache Struts 2?

A leading open source project from the Apache Foundation. Apache Struts 2 is widely used across numerous industries for developing web applications in Java. As one of the more popular projects in the open source space, a lot of eyeballs have passed over this product. As a result of this increased scrutiny, numerous vulnerabilities have been uncovered in its different versions. The CVE database shows it to have over 68 vulnerabilities to its name.

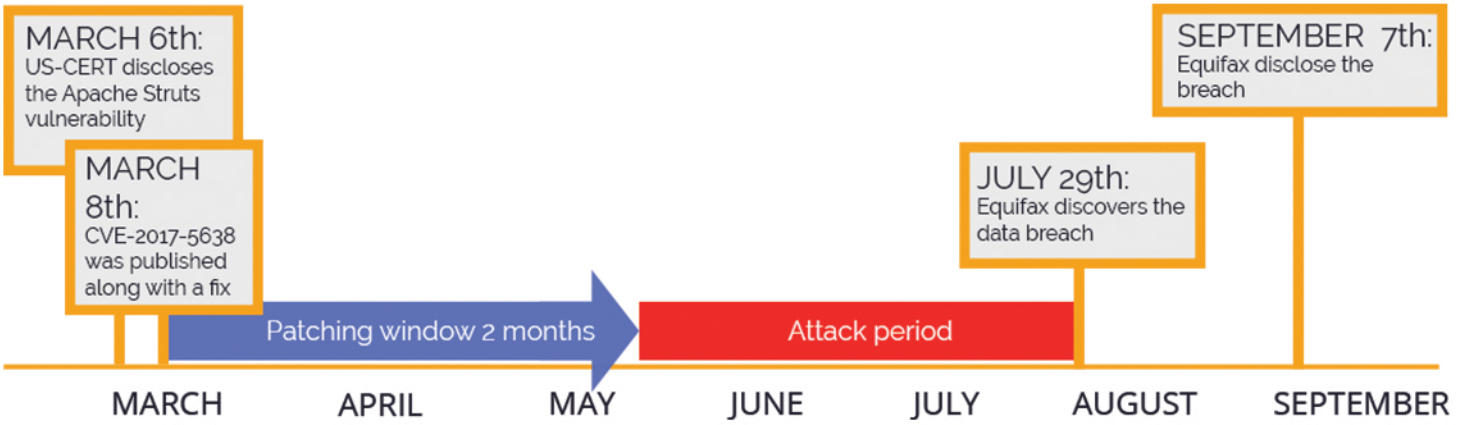
What happened?

In September 7th, 2017 Equifax announced a data breach in which financial and personal data on 145M US consumers were obtained.

Attackers exploited a known vulnerability in the Apache Struts 2 project, breaching Equifax's web application to steal personal identifying information (PII). The hack is believed to have occurred sometime in May. At that time, the vulnerability (CVE-2017-5638) in Apache Struts 2 was already disclosed to the public and many hackers were exploiting it en-mass on different application across the world.

Reports indicate that the breach ran undetected by Equifax until July. This breach has been labelled as the largest and most severe corporate data breach in history since almost a half of the US population was impacted and due to the sensitivity of the information.

The timeline and facts



Key Dates for the Equifax Breach Saga:

March 6th: A cybersecurity arm of the U.S. Department of Homeland Security, the US-CERT, "identified and disclosed" the Apache Struts vulnerability after chatter on the Darknet were found discussing how it could be exploited by hackers.

March 8th: CVE-2017-5638 was published as a known vulnerability, along with a fix which called to replace version. At the same day of the announcement, several security analysts reported the bug was under mass attack by hackers who were exploiting the flaw to install rogue applications on Web servers.

May - July 29th: Equifax believes that their application was breached sometime between May and July, which means the attackers exfiltrate the massive amount of personal identifiable information without anyone detecting the hack in real-time.

September 7th: Equifax makes their public disclosure of the breach, setting off the firestorm of criticism for their haphazard handling of the affair.

What should we learn from this?

In looking back at the attack, there are two main lessons we should all learn.

The most glaring point of the whole debacle is the fact that the breach could have been prevented had Equifax managed their open source usage. Companies need to understand the risk in using open source components with known vulnerabilities, since these vulnerabilities are known to all – including hackers.

The second lesson is that detecting vulnerable open source components can only be done using dedicated tools for open source security. According to reports, Equifax was employing security scanning solutions for testing their internally written code, which failed to detect the vulnerable component and recommend the fix. Open source is distinct from proprietary code and needs a different approach from a security perspective, one that integrates intelligence from community sources and is less labor intensive for your in-house team to have to follow up on in order to secure your products.