Equifax exposed 300,000 credit card numbers in which

Sociology, Identity

Equifax Inc. is a consumer credit reporting agency. Equifax collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide. On September 10, 2017, a massive cyber security incident occurred at Equifax. Private information belonging to 140 million people was reportedly stolen. The breach, was initially discovered on the 29th of July.

The information that was stolen consisted of social security numbers, addresses, driver’s license numbers, and even birthday. The breach also exposed 300, 000 credit card numbers in which some were international customers. The data breach affected thousands of American consumers as it exposed their private credit information. The data stolen could also be easily used for identity theft. The credit card agency traced the theft of 143 million Americans’ sensitive information. Their discovery revealed that the software flaw could have been fixed before the data breach and the whole scandal could have been prevented. Last year, 2016, Equifax was informed that their website was vulnerable to a cross-site scripting vulnerability. Although they were notified in 2016, they did not inform their customers until it had already happened.

By definition, Cross-site scripting (XSS) is a security vulnerability allowing a user to alter the code that an application delivers to a user which is executed in the user’s web browser. It is most commonly found in web applications affecting the user’s browser, but also possible in other applications with embedded web content, such as an interactive “ help” content viewer. When an XSS vulnerability is used as an attack vector, input sent by the attacker is insecurely processed within the application in a way that allows the attacker to alter the code sent to the victim and executed on in the web browser (" What is cross-Site scripting (XSS)? – Definition from WhatIs. Com." SearchSoftwareQuality, searchsoftwarequality. techtarget.

com/definition/cross-site-scripting). When Equifax reportedly failed to install a security fix to the flaw, the hackers took advantage of that open window, which lasted a whopping two months, to puncture the company's digital defenses. The hackers exploited this flaw after months as no action was taken in order to prevent the breach. Many of the victims criticized Equifax for how they handled the situation. Firstly, they did not notify their consumers about the threat. Secondly, Equifax did not the necessary security measures that could be used to drastically or in some cases, entirely remove the threat of cross-site scripting.

Equifax was harshly criticized for lacking strong input validation, content security policy, and output encoding. These are all controls which protect a site from cross-site scripting; Equifax did not take these measures even after they were well-informed about the threat. Input validation detects if an end user's input matches the expected format. CSP generally restricts which scripts can be ran on a given webpage. Output encoding ensures that certain characters the browser is going to receive should be treated as display text, rather than executable code.

The security experts say that Equifax should have moved faster. It is inexcusable for a company of that size with thank kind of magnitude of data to not take drastic security measures. They were widely criticized for waiting more than a month to alert and inform their customers and shareholders about the issue. The Equifax data breach comprised 143 million social security numbers. The hackers seized birth dates, addresses, driver’s license information, and credit card reports. The hackers also disputed documents with personal identifying information for around 182, 000 individuals.

Even credit card numbers for about 209, 000 individuals were seized during the breach. The data stolen could easily be utilized for identity theft. Regardless of how absurd the numbers are; the danger lies in the type of data stolen. All the data stolen was data which identified an individual.

The stolen data has the potential to cause serious damage due to seizing personal identifying information. Data breaches typically involve the theft of usernames and password, but the information leaked in this breach poses a much larger threat. The cybercriminals are highly likely to use the stolen Equifax data to commit identity theft. The breach exposed the necessary information for criminals to apply for loans, credit cards, and even transfer money.

The hackers have access to the actual funds that these account are worth and are capable of using them for their own personal gain. There is currently no evidence of the data being used, experts say that the hackers are being very cautious with the data due to the ongoing investigation.