Equifax Data Breach: Security Brief

September 2017

On September 7, 2017, a large-scale data breach was announced. Equifax, one of the three major credit reporting agencies, revealed that a data breach may have affected 143 million consumers by exposing Social Security numbers and other personal information. This equates to 44% of the entire U.S. population that had their personally identifiable information (PII) stolen. Here's what we know so far, and what actions you can take.

How the Breach Happened

While Equifax's communication of the breach and who were affected have not been very clear, it was revealed that between mid-May and July of this year, hackers gained access to customer data through a vulnerability in a web application.[1] Up to 209,000 credit card numbers and 182,000 other PII data points like Social Security numbers, birth dates, addresses and driver's license numbers were stolen. Equifax learned of the breach on July 29, and hired an outside forensics firm to investigate further.[2]

The company also revealed that some UK and Canadian residents have also been affected. Equifax's lack of information is alarming considering they knew about the attack in July, yet took two months to publicly announce the breach with no information about how it occurred.

Some reports have now identified an open-source software distribution, Apache Struts, as the culprit for the breach.[3] Apache Struts is a popular open-source software programming Model-View-Controller framework for Java; the security flaw in question was patched in March, 2017. The question is, did Equifax update the software, or did the hackers find a way into an unpatched Equifax server? Until Equifax reveals more details, the blame remains unclear. What is clear is that many consumers fear their personal information may be used against them, whether it be financial accounts being accessed by hackers, or someone filing an illegitimate tax return in their name. If hackers have your personal information, they can do anything.

untangle

What You Can Do

Equifax has offered a site that is supposed to easily provide a quick answer as to whether your information has been compromised. Unfortunately, the site is delivering inconsistent results, and may not be providing accurate statements.[4] Here are some things that you can try:

- **Check credit reports** – Only use known credit report agencies to check your credit. Report any suspicious activity as fraud.
- **Place a credit freeze or a fraud alert on your file** – This action will prevent hackers from opening up any new accounts in your name.
- **Keep an eye on your bank and credit card accounts** - If you see charges that you didn't make, your account has been compromised.
- **File taxes early** - Ensure hackers cannot submit a tax return in your name by filing early.

If your information has been compromised, make sure you take immediate action to stop hackers from gaining access to your financials, opening up accounts in your name, and stealing your identity.

Aftermath

Unfortunately, this won't be the last data breach to occur. Many in Congress are calling on Equifax to answer to the breach, which could lead to new legislation to ensure consumer data is properly secure and protected.[5]

Resources

1 https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/

2 https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/

3 http://www.zdnet.com/article/equifax-blames-open-source-software-for-its-record-breaking-security-breach/

4 http://www.zdnet.com/article/we-tested-equifax-data-breach-checker-it-is-basically-useless/

5 http://fortune.com/2017/09/08/equifax-what-to-do/

About Untangle

Untangle is an innovator in cybersecurity designed specifically for the below-enterprise market, safeguarding businesses, home offices, nonprofits, schools and governmental organizations. Untangle's integrated suite of software and appliances provides enterprise-grade capabilities and consumer-oriented simplicity to organizations with limited IT resources. Untangle's award-winning network security solutions are trusted by over 40,000 customers around the world. Untangle is headquartered in San Jose, California. For more information, www.untangle.com.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

Untangle, Inc.
100 W. San Fernando St., Ste. 565
San Jose, CA 95113
www.untangle.com