The 2017 Equifax Hack: What We Can Learn

Alexa Helen Drenick
School of Engineering
California State Polytechnic University
San Luis Obispo, CA
Email: adrenick@calpoly.edu

I. Introduction

Recent high profile cyber security attacks have brought computer security into a place of importance in the minds of both consumers and companies [1]. As attacks become increasingly common [2] and publicized [3], how companies prevent, prepare for, and react to cyber-attacks could become a distinguishing factor. Cyber-attacks can cause not only a loss of revenue to the attacked company, but more importantly, a loss of reputation [4], so by setting ourselves apart from the lax security practices of the companies surrounding us [5], we can stand out as a defendant of privacy and proponent of excellent security practices. We have an obligation to our users to keep their data as secure as possible, and to do so, we must learn from the past and look to the future to predict how to best keep our services secure. A particularly relevant example is the 2017 attack on Equifax.

II. Technical Information

The vulnerability that led to the attack on Equifax was in the outdated version of Apache Struts Equifax was using [6]. Apache Struts is an open source model-view-controller framework commonly used in Java based web applications. The vulnerability allowed for a technique called OGNL injection [7]. OGNL (Object-Graph Navigation Language) is used to set object properties and allow execution of methods in Java classes [7] and is prevalent throughout the Apache Struts framework [6]. The vulnerability was an issue with the Jakarta Multipart parser plugin the Equifax server utilized [6]. In the version of Apache Struts used by Equifax, this parser had incorrect exception handling and error-message creation during failed file uploads [8]. This issue allowed attackers to attach code in a Content-Type HTTP header and therefore remotely execute malicious code [6].

A proof of concept of this attack was available publicly March 7, 2017 [9] and on March 8, 2017 the U.S Department of Homeland Security, Computer Emergency Readiness Team notified Equifax that they needed to patch vulnerable versions of their software [10]. On March 9, Equifax notified their security department that they were required to administer the patch within 48 hours [10]. The story should have ended here, but the vulnerable Apache Struts version was not identified and patched. On March 15, Equifax's security department ran scans, but the scans did not identify the Apache Struts vulnerability. The attack began on May 13 and was not discovered until July 30 [10]. Throughout the attack, the personal identifying information of approximately 145.5 million US consumers was accessed [11].

As if the entirely preventable sensitive information leak wasn't enough, Equifax's disorganized and delayed response made matters worse [12]. Equifax took six weeks to publicly release information about the attack [13], leaving consumers unknowingly vulnerable to various forms of identity theft [14]. Equifax then further exhibited their faulty internal security practices in the website they created for consumers to check if they were impacted or not, which required the person's last name and last six digits of their social security number. First of all, Equifax put the site up on a different domain (equifaxsecurity2017.com) instead of creating pages under their main trusted domain [11]. This left consumers vulnerable to phishing attacks: websites that maliciously posed as

Equifax to collect the information people would supply to Equifax to determine if they were vulnerable. This was such an issue that Equifax themselves tweeted an incorrect phishing link four times. Luckily this site was only created for research purposes, but the fake site had at least 200,000 page loads and indicated that Equifax deviating from their trusted domain was a poor security decision [15]. Even if customers did get to the correct site to check if they had been impacted, customers reported that they would get contradictory responses when they inputted their information on a computer and on mobile phones or inconclusive responses saying to check back. One user even input random information into the site and still got back the answer to check back later [16]. Although Equifax offered free credit monitoring in the wake of this event, most customers were unable to load the website to do so [17]. To make matters even worse, this site incorrectly handled TLS certificate revocation checking [12]. As stated by the former Equifax CEO himself, "The rollout of these resources should have been far better, and I regret that the response exacerbated rather than alleviated matters for so many" [10].

III. Impact

With the number of people impacted reaching over 145.5 million, the impacts of this attack are startling [11]. This number represents over 44 percent of the US population, but if children and people without credit histories are removed, this attack means that about half of the US population using credit services are at risk of fraud, which is causing some to call this attack the worst leak of personal information to date [18]. The leaked information leaves those impacted susceptible to two types of fraud: account takeover, where a malicious agent takes control over current accounts by using stolen personal information to assume identity, and full identity takeover, where a malicious agent uses personal information to open new false accounts [19]. A month after the hack, credit card fraud spiked, and many blame the Equifax hack [20]. Since the stolen information, social security numbers in particular, doesn't expire, there is no end in sight to risk of fraud [19].

The impact of this attack goes beyond just those whose information was stolen, cyber security incidents related to property theft often induce significant aggregate costs to the economy [4]. At least $3.46 billion worth of market value has been exacted since the attack was announced [21]. Equifax stock fell 31% in the months following the breach disclosure [22].

But the cost to Equifax won't just be in market losses. Since the breach, Equifax's CEO, CIO, and CISO all stepped down [12]. Equifax has also been served over two dozen class-action lawsuits and a lawsuit from the state of Massachusetts [10]. Arguably the worst cost to Equifax will be in loss of reputation. It's been shown that a company's reputation is strongly affected when a cyber-attack is widely reported in media outlets, involves leaking sensitive information, and is publicly traded [4]; all of which apply to this Equifax breach. As stated by Marc Dunn, "Equifax's only job in life was to safeguard data" [23], and now they've lost all credibility of their capability to do that [12].

IV. Mitigation Techniques

This breach should serve as a reminder of the importance of good security practices and training throughout all areas of an organization. As stated by the former CEO of Equifax, "the breach occurred because of both human error and technology failures", but it would seem poor leadership and a corporate under-emphasis on security were also major factors [12].

Although the basis of this attack was in unpatched third-party open source software (OSS), it exposes an overall issue with development processes. Since OSS is often used throughout the application stack, it's critical that third-party component oversight is methodical and well managed. If security practices are maintained throughout the entire development process, code can be secure from the inside out instead of relying on insufficient firewalls, incorporated OSS can be monitored and tracked, and design decisions can be made to address potential security issues [6].

To achieve these changes, security needs to be taken out of isolation and brought into cooperation with more areas: development, IT, operations and legal teams need to partner with the security team. Development must provide a list of all OSS used so security can monitor known vulnerabilities and track components of code. Operations must have a defined process for applying patches and communicating with customers [6].

Security must also be a continuous process throughout the entirety of the development cycle: design, development, installation, and deployment. Security focused code reviews can be conducted during development, static analysis should be executed during development, and penetration testing should be completed before deployment. Software Composition Analysis technology can be used to consistently monitor code by automatically generating vulnerability alerts and what OSS is in the code base [6].

To prevent issues with missing patches and exposure to known vulnerabilities, OSS use should be examined on many levels. The OSS inventory should be well defined including all versions in use, where OSS exists in the code base, how the OSS is used, and vulnerabilities within versions in use. Who is responsible for monitoring and upgrading versions should be well defined and there should be a specific policy for OSS use and approval [6].

V. Related Attacks

The discussed attack on Equifax is not an isolated incident, in 2017 alone 41 large companies have had information breached as the result of a cyber-attack [2]. In the attack on Equifax, the attackers had the upper hand: since Apache is open-source, they had access to the code they were attacking, and they had access to a published proof of concept for the attack they were executing [9]. Some experts believe that OSS is more vulnerable to attack then commercially developed software since hackers then have access to the source code they are trying to exploit. For example, Teardrop was a denial of service attack reliant on an intimate knowledge of Linux's implementation of the IP stack, which was allowed by Linux's open-source nature [24].

Although exposure to source-code may make OSS easier for hackers to attack, the number of developers looking for vulnerabilities and suggesting solutions to them is much greater [24], which is a strength that must be leveraged. In the case of the Equifax hack, a patch to the exploited vulnerability was immediately available, it was an issue of executing the patching process within the company [10]. According to a survey conducted on hackers, about 10% of security breaches are due to unpatched software [25]. Until companies solidify updating and patching protocol, attackers will maintain the upper hand of having known vulnerabilities to exploit. For example, the WannaCry exploits, numbering nearly 45,000 attacks, exploited a vulnerability in obsolete versions of Windows [26]. Until security practices and attitudes change, there is no reason these types of attacks will cease to succeed and impact businesses and customers worldwide.

VI. Conclusion

The 2017 Equifax hack exploited a vulnerability within a third party open source framework that had a safe patch available. Not only is Equifax at fault for allowing known vulnerabilities within their products, but also for their disjointed and poorly coordinated effort to triage. To prevent financial and reputation threatening attacks such as this one we must redesign our development cycle to include security checks throughout, integrate all teams with the security team, and prepare a plan and procedure for responding to potential exploits. Although these changes will require an attitude shift and training efforts, the potential business impact of an information breach is far too large of a risk to ignore.

REFERENCES

[1] J. Loughnane, “The Role of Resolution in Resiliency,” *American Bankruptcy Institute Journal,* vol 37, no. 2 pp. 28-29, February 2018.

[2] “2017 Data Breaches - The Worst Breaches, So Far,” *IdentityForce*, 14-Dec-2017. [Online]. Available: https://www.identityforce.com/blog/2017-data-breaches.

[3] A. Wells, “What's Next for Cyber Insurance?,” *Insurance Journal*, 21-Apr-2014. [Online]. Available: https://www.insurancejournal.com/magazines/features/2014/04/21/326382.htm.

[4] G. Davis, A. Garcia, and W. Zhang, “Empirical Analysis of the Effects of Cyber Security Incidents,” *Risk Analysis*, vol. 29, no. 9, pp. 1304–1316, Jun. 2009.

[5] H. Berghel, "Bruce Schneier on Future Digital Threats," in *Computer*, vol. 51, no. 2, pp. 64-67, February 2018.
doi: 10.1109/MC.2018.1451653

[6] Luszcz, Jeff. “Apache Struts 2: How Technical and Development Gaps Caused the Equifax Breach.” *Network Security*, vol. 2018, no. 1, Jan. 2018, pp. 5–8., doi:10.1016/s1353-4858(18)30005-9.

[7] H. Shah, “Analyzing CVE-2017-9791: Apache Struts Vulnerability Can Lead to Remote Code Execution,” *McAfee Blogs*, 23-Aug-2017. [Online]. Available: https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-cve-2017-9791-apache-struts-vulnerability-can-lead-remote-code-execution/.

[8] “CVE-2017-5638 Detail,” *National Vulnerability Database*, 22-Sep-2017. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[9] S. Sahu, “CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution,” *TrendLabs Security Intelligence Blog*, 09-Mar-2017. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/.

[10] E. R. Hendry, “How the Equifax hack happened, according to its CEO,” *PBS*, 03-Oct-2017. [Online]. Available: https://www.pbs.org/newshour/nation/equifax-hack-happened-according-ceo.

[11] “2017 Cybersecurity Incident & Important Consumer Information,” *Equifax*. [Online]. Available: https://www.equifaxsecurity2017.com/consumer-notice/.

[12] H. Berghel, “Equifax and the Latest Round of Identity Theft Roulette,” *IEEE Computer Society*, vol. 50, no. 12, pp. 72–76, Dec. 2017.

[13] “Equifax had 'admin' as login and password in Argentina,” *BBC News*, 13-Sep-2017. [Online]. Available: http://www.bbc.com/news/technology-41257576.

[14] M. LaMagna, “What to do now if you're among 143 million Americans affected by Equifax data breach,” *MarketWatch*, 10-Sep-2017. [Online]. Available: https://www.marketwatch.com/story/are-you-one-of-the-143-million-customers-in-the-equifax-data-breach-do-this-now-2017-09-08.

[15] L. H. Newman, “All the Ways Equifax Epically Bungled Its Breach Response,” Wired, 24- Sep-2017. [Online]. Available: https://www.wired.com/story/equifax-breach-response/.

[16] B. Krebs, “Equifax Breach Response Turns Dumpster Fire,” *Krebs On Security*, 08-Sep-2017. [Online]. Available: https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/.

[17] B. Krebs, “Equifax Breach: Setting the Record Straight,” *Krebs on Security*, 20-Sep-2017. [Online]. Available: https://krebsonsecurity.com/2017/09/equifax-breach-setting-the-record-straight/.

[18] D. Goodin, “Why the Equifax breach is very possibly the worst leak of personal info ever,” *Ars Technica*, 07-Sep-2017. [Online]. Available: https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/.

[19] L. Strum and D. Cooney, “Affected by the Equifax hack? Here's what to do now,” *PBS*, 13-Sep-2017. [Online]. Available:

https://www.pbs.org/newshour/nation/affected-equifax-hack-heres-now.

[20] L. Fickenscher, “Credit card fraud spikes after Equifax cyber-attack,” *New York Post*, 08-Sep-2017. [Online]. Available: https://nypost.com/2017/09/08/credit-card-fraud-spikes-after-equifax-cyber-attack/.

[21] T. Kilgore, “Equifax's data breach costs investors a lot more than it will cost the company,” *MarketWatch*, 11-Sep-2017. [Online]. Available: https://www.marketwatch.com/story/equifaxs-data-breach-costs-investors-a-lot-more-than-it-will-cost-the-company-2017-09-11.

[22] V. Reklaitis, “Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap,” *MarketWatch*, 14-Sep-2017. [Online]. Available: https://www.marketwatch.com/story/equifaxs-stock-has-fallen-31-since-breach-disclosure-erasing-5-billion-in-market-cap-2017-09-14.

[23] J. Gershman, “Equifax could pay for data breach in court,” *MarketWatch*, 13-Sep-2017. [Online]. Available: https://www.marketwatch.com/story/equifax-could-pay-for-data-breach-in-court-2017-09-13.

[24] S. A. Hissam, D. Plakosh and C. Weinstock, "Trust and vulnerability in open source software," in *IEE Proceedings - Software*, vol. 149, no. 1, pp. 47-51, Feb 2002. doi: 10.1049/ip-sen:20020208

[25] “Hacker Survey Report,” *Thycotic*, 2017. [Online]. Available: https://thycotic.com/wp-content/uploads/2013/03/BlackHa_Hacker_Survey_Report_2017.pdf.

[26] D. Gayle, A. Topping, I. Sample, S. Marsh, and V. Dodd, “NHS seeks to recover from global cyber-attack as security concerns resurface,” *The Guardian*, 13-May-2017. [Online]. Available: https://cyber-peace.org/wp-content/uploads/2017/05/NHS-seeks-to-recover-from-global-cyber-attack-as-security-concerns-resurface-_-Society-_-The-Guardian.pdf.