Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	2136249

Module Title & Code	*WM142 – Information Risk Management*
Module Owner	*Peter Norris*
Module Tutor	*Alexandra Samantha Driscoll*
Module Marker	*Alexandra Samantha Driscoll*
Assesment type	*Essay*
Date Set	*3rd November 2021*
Submission Date (excluding extensions)	*3rd December 2021*
Marks return date (excluding extensions)	*14th January 2022*
Weighting of mark	*30%.*

Assessment Detail	*Please see below*
Additional details	*The wordcount is 2,000 words.*
Module learning outcomes (numbered)	*1 – Apply a relevant risk management approach to a given organisation or scenario* *2 – Analyse the organisational consequences that result from inadequate information risk management*
Learning outcomes assessed in this assessment (numbered)	*2 – Analyse the organisational consequences that result from inadequate information risk management*
Marking guidelines	

Task	Mark
1: Identify a data breach that occurred within an organisation, and that it is OK to disclose, and provide a brief timeline of events.	25
2: List any relevant information risksyou believe are responsible for the data breach. Pick one information risk and identify and discuss its components (asset affected, vulnerability, threat, threat actor, impact, and likelihood).	25
3: Discuss any potential consequences the organisation or asset stakeholders could have faced. Your answer should discuss if any of the principles of information security were affected.	40
4: Provide a variety of references from a variety of sources, including academic sources	5
5: The assignment should be presented in an essay style with suitable headings. Marks will be awarded for presentation, including spelling & grammar	5
TOTAL:	100

	Please see below for a more detailed marking scheme
Submission guidance	*The assignment should be submitted as a single pdf file via tabula (https://tabula.warwick.ac.uk).*
Academic Guidance	*Academic guidance to be provide throughout the module.*
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

Equifax Incompetent Handling of Events in 2017 data Breach

WM142 – Information Risk Management (BSc Cyber Security)

Alexandra S. Driscoll

University of Warwick

Contents

Cybersecurity attacks such as data breach incidents occur frequently in the corporate world, they are spread around by media articles to inform the public about them, detail reports are made subsequently to analyse the organisation effectiveness when handling and managing data breach crisis. The UK National Cyber Security Centre ("NCSC") describes a data breach as; "An incident where data, computer systems or networks are accessed without previous consent" (NCSC, 2016). The core of cybersecurity is to protect and maintain the confidentiality, integrity, and availability (CIA) of sensitive information (DNV, 2018). As a result, when these types of incidents happen it often cause significant impact loss for both organisation and customers as their information is compromised. Therefore, effective communication and adherence to policy is crucial for a successful indent handling response and business management for the organisation reputation and survival.

Background

Equifax was affected by a data breach on the 7th of September 2017, which resulted in the leakage of personal identifiable information ("PII") for more than 145.5 million people worldwide due to a single known vulnerability inside a software called Apache Struts 2 – open-source software used in web applications - which was found to be running on three different systems. Equifax handling response to the event was considered "inadequate and hampered by Equifax's neglect of cybersecurity" by the United State Senate (Portman and Carper, 2019) because of its incompetence of not securing their systems appropriately and follow conventional standards (NIST cybersecurity Framework) like their major credit report agencies competitors ("CRA"), Experian and TransUnion. The breach led the company into public shame ruining their reputation and having to fire top executives like their CEO, CIO and CSO. As well as having to pay massive penalties to governmental agencies such as the FTC, CFPB and having to update their policies.

Timeline of Events of Data Breach.

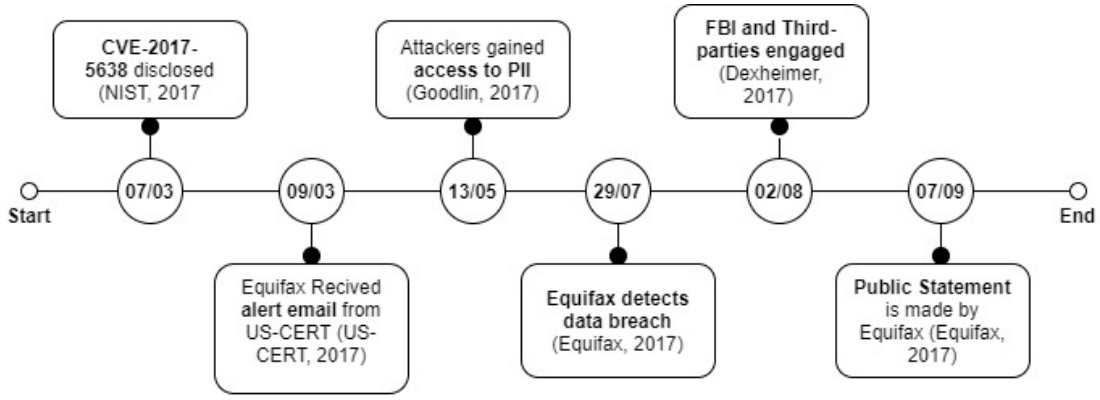


Figure 1 - Equifax Data Breach Timeline (Miguel A. L., 2021)

Figure 1 shows the most relevant events during Equifax data breach in 2017. On the 7th of March of that year, the National Institute of Standards and Technology ("NIST") disclosed the CVE-2017-5638 vulnerability related to the Apache Struts 2 framework used in three different Equifax systems at the time, scoring the patching priority to be CRITICAL "10/10" – the National Vulnerability Database ("NVD") uses this score system to give organisations a way of classifying vulnerabilities by priorities - (NIST, 2017). The Department of Homeland Security ("DHS") sent an email to major corporations like Equifax regarding the vulnerability due to ease of exploiting it (US-CERT, 2017). Equifax received this email on the 9th of March by their Global Threat and Vulnerability Management (GTVM) where they forward it to the department in charge of dealing with threats and vulnerabilities, - which consists of four hundred plus employees - due to Equifax policy, the team directed patching within forty-eight hours, scans were ran on the same day due to the nature of the vulnerability, however no threats were found (Sussman, 2017).

From May 13th to July 29th the attackers gained unauthorised access to Equifax Automated Customer Interview System ("ACIS") system conducting more than nine thousand queries against fifty-one different databases. It was until then (July 29th, 2017) that Equifax became aware of the attack. On August 2nd Equifax informed the FBI and a third-party cyber security organisation named Mandiant to conduct a forensic review (Mandiant Security, 2017). Equifax made the data breach attack public on September 7th 2017 stating that personal identifiable information ("PII") for more than 144.5 million people worldwide were leaked form Equifax databases (CAE in Cybersecurity Community, 2020).

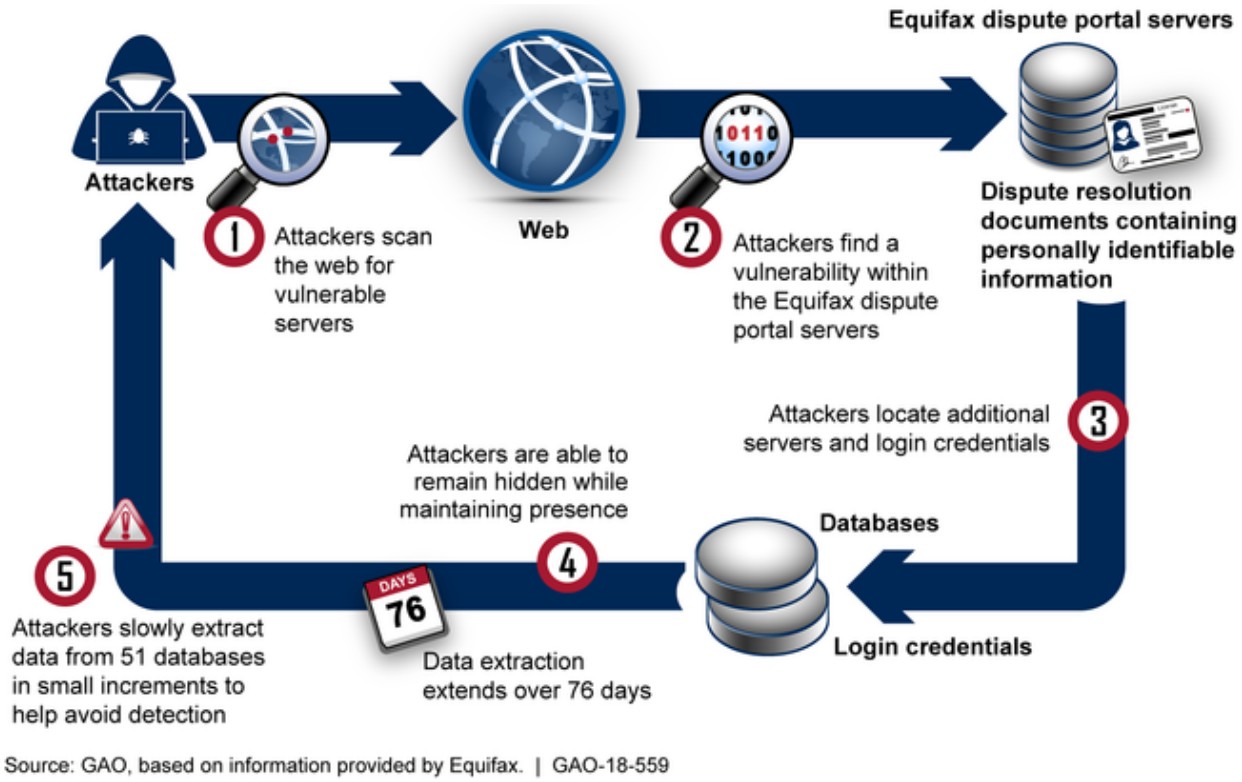


Figure 2 - How Attackers Exploited Equifax's Vulnerable Systems (GAO, 2018)

Equifax's Information Risks

Consumer reporting agencies (CRA) like Equifax are required to follow federal laws and governmental regulations for the "protection, collection and use of customer credit and related information" (U.S Congress, 2018) shown in figure 2. In the United States, the Federal Trade Commission ("FTC") and the Consumer Financial Protection Bureau ("CFPB") are the agencies in charge of regulating these organisations to prevent anti-competitive, misuse of costumer data but also offers guidance to consumers to make informed financial decisions ("FTC," 2013). To ensure compliance, the agencies operate an enforcement program, aimed at large corporations like Equifax to limit the distribution, content and manipulation of consumer credit reports and also it allows customer access their credit by enforcing the Customer Protection Act (FTC, 2018). The violation of the FCRA and CFPB can result in supervision, internal investigations, and civil penalties (Portman and Carper, 2019).

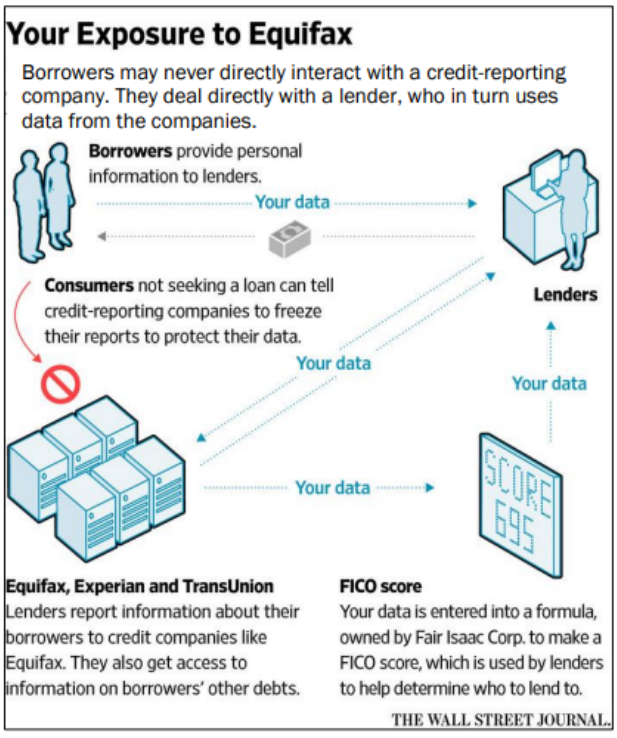


Figure 3 - Consumer Information Processed by Equifax (McMillan, 2017)

Equifax was Aware of its Cybersecurity Weaknesses.

Before 2015, Equifax did not have any official policy associated on how to patch known cybersecurity vulnerabilities on their systems, meaning there was no clear document outlining the responsibilities and/or guidance required to perform scans nor pathing vulnerable systems within the organisation, that meant that the company had no way of telling which systems were vulnerable systems or which had to be updated and patched (Richard F. Smith, 2017). It was until the former Chief Security Officer ("CSO") – Susan Mauldin – along with the Chief Information Officer ("CIO") - Jun Ying – worked together to produce Equifax's Patch Management Policy in April 2015 (Portman and Carper, 2019).

On October 28th, 2015, Equifax contracted a third-party cybersecurity organisation to perform an internal analysis to assess their effectiveness for its system configuration and patch management. The purpose for the audit was to; [1.] Assess the controls in place, [2.] Fixate configuration issues and compromised patches. [3.] Make recommendations to improve security. The conclusion of the audit was that "current patch and configuration management controls are not sufficiently designed to

guarantee Equifax systems are securely configured and patched on time" (Portman and Carper, 2019).

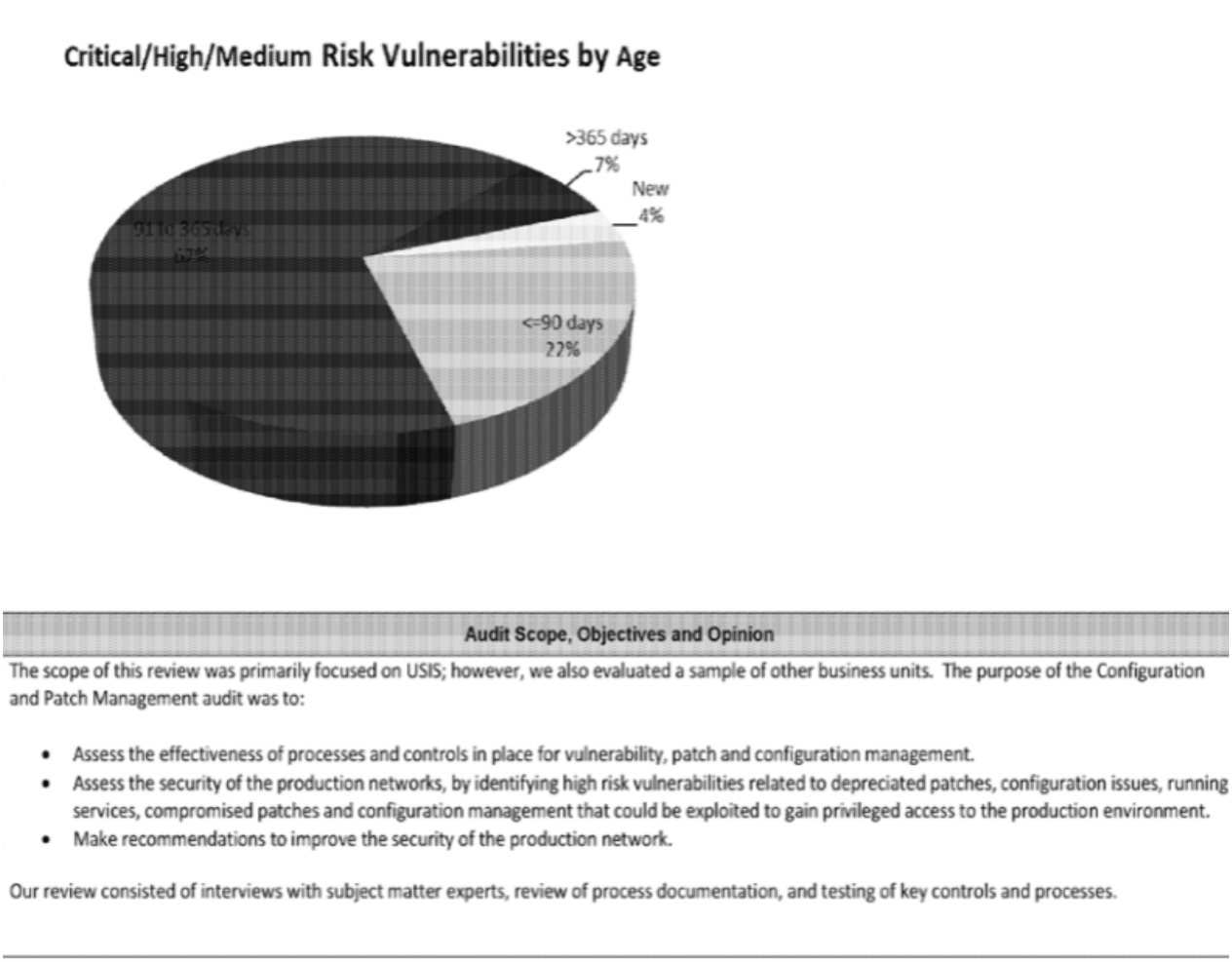


Figure 4 - Audit Vulnerability Results (Portman and Carper, 2019).

Figure 3 shows the results of the Audit performed in 2015, which states that there were "over 8,500 vulnerabilities" of which "over 1,000 classifieds as critical/high/medium" and "over 7,500 classified as critical/high" vulnerabilities affecting close to 22,000 systems, out of those "75% of the external and 93% internal vulnerabilities were over 90 days old".

a. Equifax Did Not Follow its Own Patching Schedule.

Patch Category	Patch to Deployment Times
Critical	"To Be installed within 48 hours from the time of release"
High Risk	"To be installed within 30 days from time of release"
Medium Risk	"To be released within 90 days from time of release"
Low Risk	"To be installed within the normal patching rotation (within a year)"

b. *Figure 5 – Priority Patch Categorisation (Equifax, 2019)*

One of the main reasons for the result of the audit is the fact that Equifax did not patch vulnerable systems within the timeframe stated in their policy, as shown by the audit. For example, critical vulnerabilities founded, existed for over 90 days without patching, which is against their own policy as shown in Figure 4 which states that critical vulnerabilities should be patched "within 48 hours". This lack of remediation of vulnerabilities "created a security exposure and enabled attackers to compromised Equifax system", making customer data at risk (Portman and Carper, 2019).

c. Equifax **used a "Honor System" for patching.**

By the start of 2017, when the data breach occurred Equifax had no formalised method of validating successful installation patches, instead they used what is known as a "Honor System" whereby the IT team in charge of installing a patch would notify the security team once installation was complete. The security team will then scan their systems that were "patched" to determine if the installation was completed, if the scan did not alert of any vulnerability, then it was assumed that a patch was successfully applied. According to Equifax's former Countermeasures Manager, that way of approaching patching is not advisable, instead he recommended the implementation of

a centralised system that would verify the scans before determining that “no further action” was needed.

d. Equifax Lacked an Information Technology (“IT”) Assets Inventory.

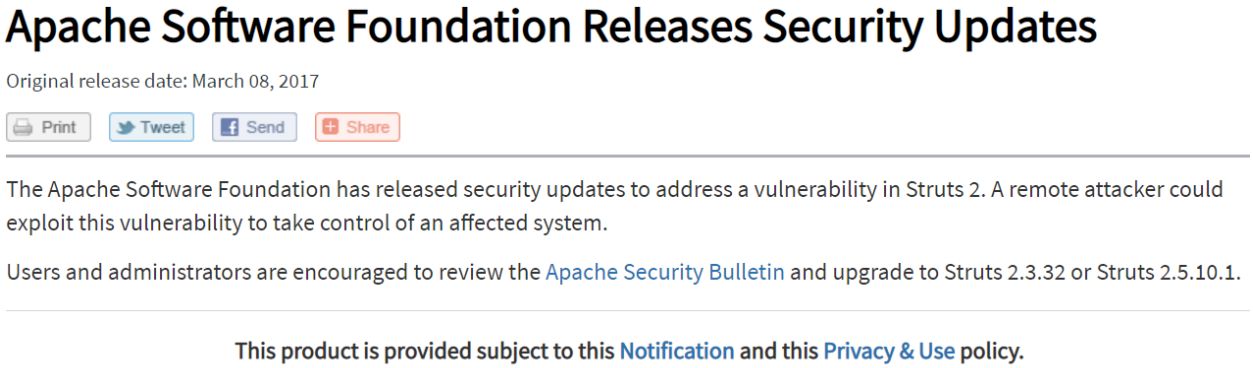
However, the main reasons the audit found that many vulnerabilities is because “Equifax lacked a complete Information Technology (“IT”) asset inventory”, which explains the reason why Equifax took a long time to respond and act to the email sent by the **DHS** stating the Apache Struts 2, vulnerability as the company did not had the means to detect whether or not they were running that specific software on their systems due to their lack of resources, which “makes it difficult to ensure systems are patched in a timely manner” (Portman and Carper, 2019).

By having a complete asset inventory, the organisation can better protect itself from cyber threat actors, because “an organisation can only defend their assets that it has identified” (Equifax, 2018), meaning that without it, information assets like customer “**PII**” data become at risk to be exposed and used without the owner consent for malicious purposes by threat actors. It creates a vulnerability for the company when an attack occurs, as they would not be able to act rapidly, potentially impacting all aspects of the CIA triangle.

In the 2017 data breach, Equifax was unable to detect it mainly because, they had no idea that their SSL certificates – “a global standard technology that enables encrypted communication between a browser and server” (Verisign, 2021) - were expired, these certificates must be active to allow a website to decrypt and **monitor** incoming network traffic, Equifax SSL certificates for its dispute portal (where CVE-2017-5638 was present) were expired in November 2016, it was not until eight

months later when they renew their certificates on July 29, 2017, that they found out about the attack, Equifax was able to trace back the attackers IP address to China, where they do not operate, but by then it was discovered that the attackers had already been 76 days inside their systems. Once the attackers got accessed into the dispute portal, – where credit report information about consumers were stored – they started to extract sensitive information such as: full names (including nicknames), date of birth, current and former addresses, phone numbers, driver licenses and full social security numbers, along with UNENCRYPTED **usernames** and **passwords** for various databases, which combined accumulated for more than **145 million** American customer records (~**44%** of the population). Unauthorised access was possible due to Equifax's decision not to segment its systems by limiting access to other systems once a user was in the dispute portal, a graphical example is shown in Figure 2. Their explanation was "to support efficient operations and functionality", however, this was inconsistent with the cybersecurity NIST framework standard (nicole.keller@nist.gov, 2013).

Equifax Response to the Vulnerability facilitated the Breach



Apache Software Foundation Releases Security Updates

Original release date: March 08, 2017

Print Tweet Send Share

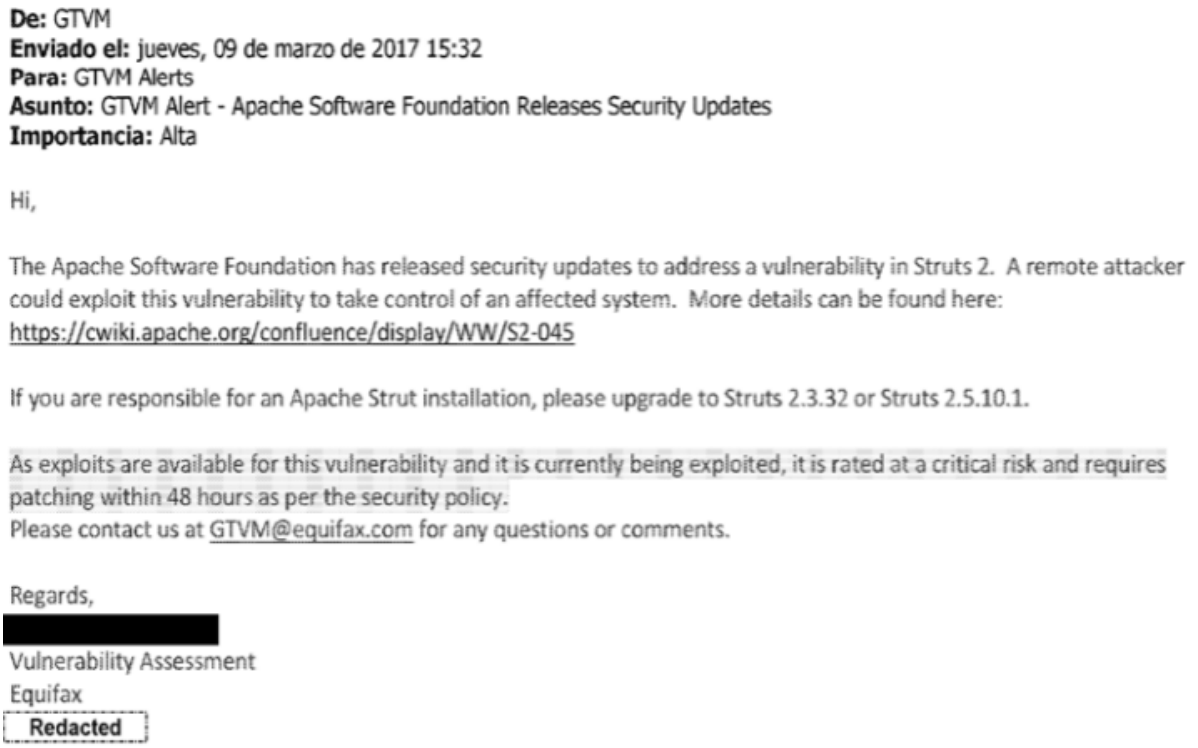
The Apache Software Foundation has released security updates to address a vulnerability in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system.

Users and administrators are encouraged to review the Apache Security Bulletin and upgrade to Struts 2.3.32 or Struts 2.5.10.1.

This product is provided subject to this Notification and this Privacy & Use policy.

Figure 6 - Vulnerability Alert sent by DHS (US-CERT, 2017)

On March 8, 2017, the DHS U.S-Computer Emergency Readiness Team ("US-CERT") sent a public alert (shown in Figure 6) after learning of the Apache Struts 2 vulnerability now known as CVE-2017-5638 by the NIST assigning the highest severity score, a 10, to it (US-CERT, 2017). This means, that the vulnerability was widely known, Equifax also received an email by the US-CERT that same way and it was forwarded to more than 400 employees from their cyber security team (Ping Wang, 2018) shown in Figure 7, however the developer in charge of that specific system did not receive the notice to upgrade their systems to a safter version.



De: GTVM
Enviado el: jueves, 09 de marzo de 2017 15:32
Para: GTVM Alerts
Asunto: GTVM Alert - Apache Software Foundation Releases Security Updates
Importancia: Alta

Hi,

The Apache Software Foundation has released security updates to address a vulnerability in Struts 2. A remote attacker could exploit this vulnerability to take control of an affected system. More details can be found here:
https://cwiki.apache.org/confluence/display/WW/S2-045

If you are responsible for an Apache Strut installation, please upgrade to Struts 2.3.32 or Struts 2.5.10.1.

As exploits are available for this vulnerability and it is currently being exploited, it is rated at a critical risk and requires patching within 48 hours as per the security policy.
Please contact us at GTVM@equifax.com for any questions or comments.

Regards,
[redacted]
Vulnerability Assessment
Equifax
Redacted

Figure 7 - Email sent by the US-CERT (U.S Congress, 2018)

The likelihood of the vulnerability from being exploited were extremely high as the tools to exploit the March 2017 Apache Struts Vulnerability were publicly available to use (Woo, 2017) four days before even the patch came out on the GitHub.com – a development platform used to build software - platform. Yet, it took months for the company to fix the issue, which shows failure to implement basic cyber security standards from its own internal policies and procedures to prevent the breach from happening. Furthermore, the company did not make the breach public until September 7, 2018 (AVA Security, 2019), which led the public unaware of the event for six events after learning about the incident, this further shows the inefficacy communication practices carried about by Equifax.

Governmental Assessments on Equifax Handling of Data Breach.

After Equifax announced the data breach to the public, the three major federal agencies; The Internal Revenue Service ("IRS"), Social Security Administration ("SSA"), and the U.S Postal Services (USPS) got involved, as these organisations used Equifax's identity verification services, each agency led an internal assessment on how the organisation handled the breach, taking various actions based on Equifax's responsibilities and how the breach affected their operations; [1.] identify affected consumers, [2.] perform an assessment on Equifax's control systems, [3.] modify contracts with Equifax, [4.] communicate with affected individuals (GAO, 2018).

Due to concerns about possible fraud of using the stolen data, the IRS and SSA obtain the list of affected individuals to match it against their own consumer list and see whether any of them were affected and look for identity fraud for those customers. Alongside with the USPS, they further performed an independent assessment on Equifax security controls on both physical and cybersecurity controls at Equifax's data centres in; Alpharetta, Georgia, and St. Louis, according to the SSA the company did not comply with the NIST standards and pose a "moderate" level of risk. Because of this both IRS and SSA made changes to the contracts in place they had with Equifax to require "prompt notification of any future breach" as well as making Equifax pay **575 million dollars** as part of settlement scheme program (FTC, 2019). Before the data breach Equifax did not need to notify them unless the systems that provided services to the federal government were involved. Furthermore, each agency made a public statement about the effects of the breach, the IRS communicated that the breach would not have any impact on taxpayers' ability to security file tax returns. The SSA published a blog-post about the steps that consumers should take to protect their Social Security Numbers (Jim Borland, 2017).

References

AVA Security, 2019. The Equifax Breach Simplified.

CAE in Cybersecurity Community, 2020. Equifax Breach as Cybersecurity Case Study.

DNV, 2018. The three-pillar approach to cyber security: Data and information protection. URL https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683 (accessed 12.1.21).

Equifax, 2018. Interview with Manager, Countermeasures.

FTC, 2019. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. URL https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related (accessed 12.1.21).

FTC, 2018. Credit Reporting [WWW Document]. Federal Trade Commission. URL https://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting (accessed 11.28.21).

FTC [WWW Document], 2013. . Federal Trade Commission. URL https://www.ftc.gov/about-ftc (accessed 11.28.21).

GAO, 2018. Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (No. GAO-18-559).

Jim Borland, 2017. Protecting Your Social Security. Social Security Matters. URL https://blog.ssa.gov/protecting-your-social-security/ (accessed 12.2.21).

Mandiant Security, 2017. Cyber Security Threat Intelligence Solutions & Managed Services [WWW Document]. URL https://www.mandiant.com/ (accessed 12.1.21).

McMillan, A.A., Michael Rapoport and Robert, 2017. ‘We’ve Been Breached’: Inside the Equifax Hack. Wall Street Journal.

NCSC, 2016. NCSC [WWW Document]. URL https://www.ncsc.gov.uk/information/ncsc-glossary (accessed 11.28.21).

nicole.keller@nist.gov, 2013. Cybersecurity Framework [WWW Document]. URL https://www.nist.gov/cyberframework (accessed 11.30.21).

NIST, 2017. NVD - cve-2017-5638 [WWW Document]. URL https://nvd.nist.gov/vuln/detail/cve-2017-5638 (accessed 11.26.21).

Ping Wang, R.M., 2018. CYBERSECURITY INCIDENT HANDLING: A CASE STUDY OF THE EQUIFAX DATA BREACH. IIS. https://doi.org/10.48009/3_iis_2018_150-159

Portman, R., Carper, T., 2019. HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH 71.

Richard F. Smith, 2017. Richard F. Smith Testimony.

Sussman, B., 2017. Day-by-Day Timeline of Equifax Breach from Former CEO.

U.S Congress, 2018. The Equifax Data Breach.

US-CERT, 2017. Apache Software Foundation Releases Security Updates | CISA [WWW Document]. URL https://us-cert.cisa.gov/ncas/current-activity/2017/03/08/Apache-Software-Foundation-Releases-Security-Updates (accessed 11.27.21).

Verisign, 2021. What is an SSL Certificate? URL https://www.verisign.com/en_US/website-presence/online/ssl-certificates/index.xhtml (accessed 11.30.21).

Woo, V., 2017. Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution. Exploit Database. URL https://www.exploit-db.com/exploits/41570 (accessed 12.1.21).