

CVE-2020-26258&26259: XStream漏洞复现

原创 蔷薇 Timeline Sec 1周前

收录于话题

#漏洞复现文章合集

70个

上方蓝色字体关注我们，一起学安全！

作者：蔷薇@Timeline Sec

本文字数：899

阅读时长：2 ~ 3min

声明：请勿用作违法用途，否则后果自负

0x01 简介

XStream基于Java库，是一种OXM Mapping 技术，用来处理XML文件序列化的框架,在将JavaBean序列化，或将XML文件反序列化的时候，不需要其它辅助类和映射文件，使得XML序列化不再繁琐。XStream也可以将JavaBean序列化成Json或反序列化，使用非常方便。

0x02 漏洞概述

编号：CVE-2020-26258,CVE-2020-26259

2020年12月14日，XStream 发布了XStream 反序列化漏洞的风险提示。

在运行XStream的服务上，未授权的远程攻击者通过构造特定的序列化数据，可造成服务端请求伪造/任意文件删除。

0x03 影响版本

Xstream <= 1.4.14

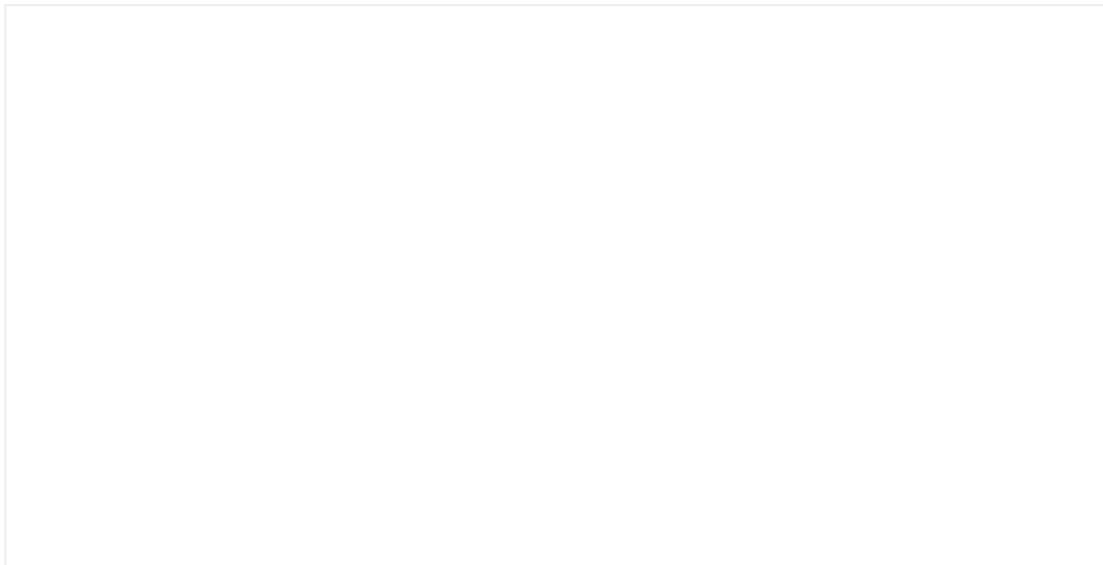
0x04 环境搭建

参考链接：

<https://github.com/jas502n/CVE-2020-26259>

使用IntelliJIDEA

在配置好maven环境以后，创建一个默认的maven项目



在pom.xml中，添加XStream依赖：

```
1      <!-- https://mvnrepository.com/artifact/com.thoughtworks.xstream/xstream -->
2      <dependencies>
3          <dependency>
4              <groupId>com.thoughtworks.xstream</groupId>
5              <artifactId>xstream</artifactId>
6              <version>1.4.14</version>
```

```
7     </dependency>
8 </dependencies>
```

到这里，我们在新建的XStream项目中引入了XStream依赖

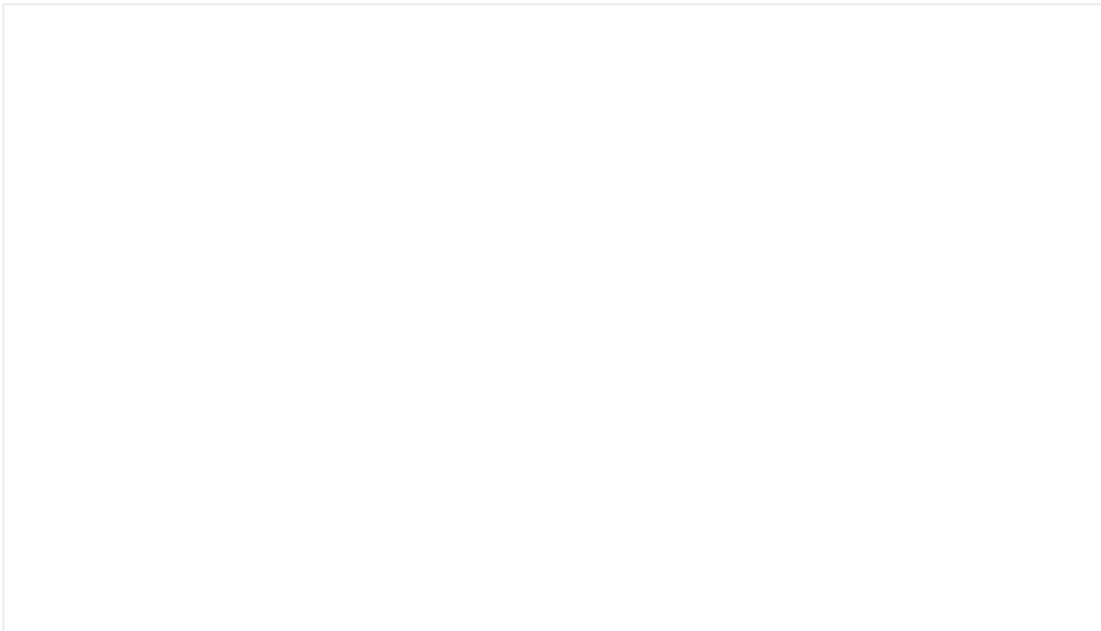
简单使用

新建一个Test.java文件，内容如下：

```
1 import com.thoughtworks.xstream.XStream;
2 import com.thoughtworks.xstream.io.json.JettisonMappedXmlDriver;
3
4 class Person//JavaBean实体类
5 {
6     private String name;
7     private int age;
8     public Person(String name,int age)
9     {
10         this.name=name;
11         this.age=age;
12     }
13     @Override
14     public String toString()
15     {
16         return "Person [name=" + name + ", age=" + age + " ]";
17     }
```

```
18
19 }
20
21 public class Test
22 {
23     public static void main(String[] args)
24     {
25         Person bean=new Person("美女",18);
26         XStream xstream = new XStream();
27         //XML序列化
28         String xml = xstream.toXML(bean);
29         System.out.println(xml);
30         //          //XML反序列化
31         bean=(Person)xstream.fromXML(xml);
32         System.out.println(bean);
33
34     }
35 }
```

运行结果，如下图所示：



到这里，我们简单使用Xstream实现了将java对象和xml文件相互转换的过程

0x05 漏洞复现

CVE-2020-26258 SSRF

在main -> java下创建一个CVE-2020-26258.java文件，代码为

```
1 https://github.com/jas502n/CVE-2020-26259/blob/main/CVE\_2020\_26258.java
```

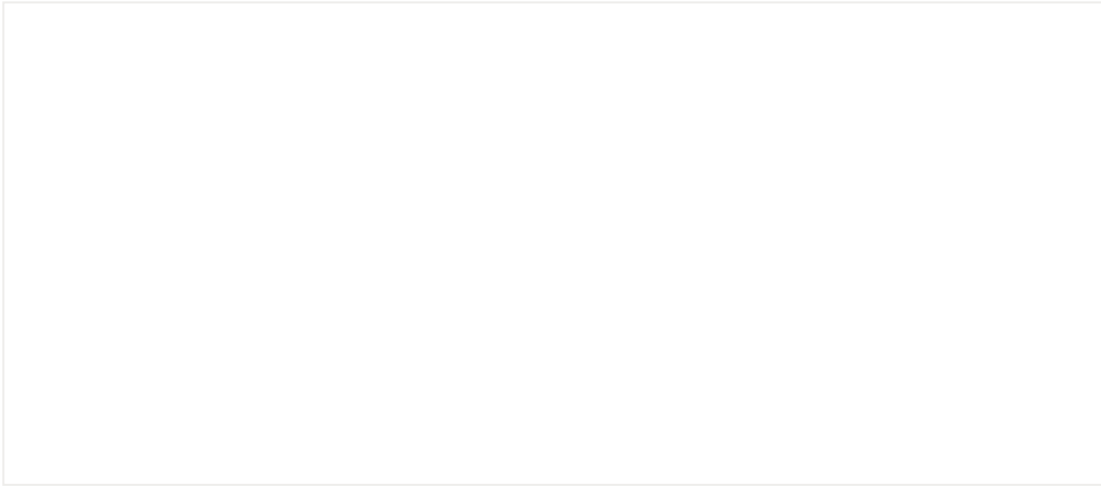
本地nc监听8989端口

CVE-2020-26259 任意文件删除

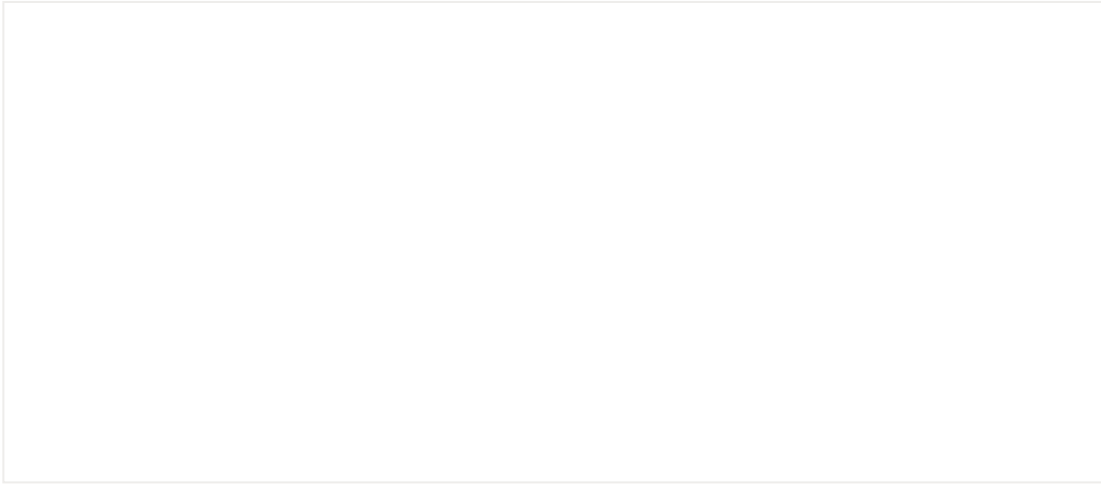
在main -> java下创建一个CVE-2020-26259.java文件，代码为

```
1 https://github.com/jas502n/CVE-2020-26259/blob/main/CVE\_2020\_26259.java
```

测试实现删除某一个文件：



运行后, ceshi.txt已被删除:



动图:



0x06 修复方式

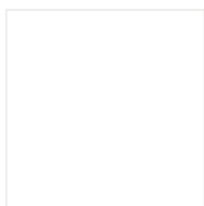
将XStream升级到最新版本。

参考链接：

<https://github.com/jas502n/CVE-2020-26259>

<https://x-stream.github.io/CVE-2020-26258.html>

<https://x-stream.github.io/CVE-2020-26259.html>



阅读原文看更多复现文章

Timeline Sec 团队
安全路上，与你并肩前行



收录于话题 #漏洞复现文章合集·70个

上一篇

CVE-2020-29436: Nexus3 XML外部实体注入复现

下一篇

骑士CMS模版注入+文件包含getshell复现

阅读原文

喜欢此内容的人还喜欢

从溯源到拿下攻击者服务器！

网络安全编程与黑客程序员

黑客入侵，服务器被当作挖矿机器！

网络安全编程与黑客程序员

我的2020

一个安全研究员