CVE-2020-26258&26259：XStream漏洞复现

原创 蔷薇 Timeline Sec
2020-12-25原文

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OXMapping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

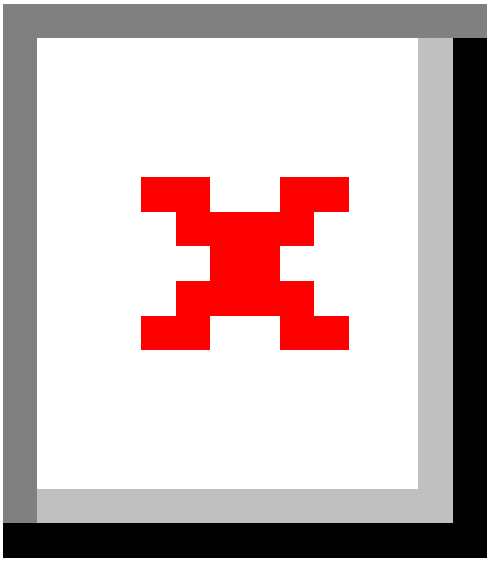
Xstream <= 1.4.14

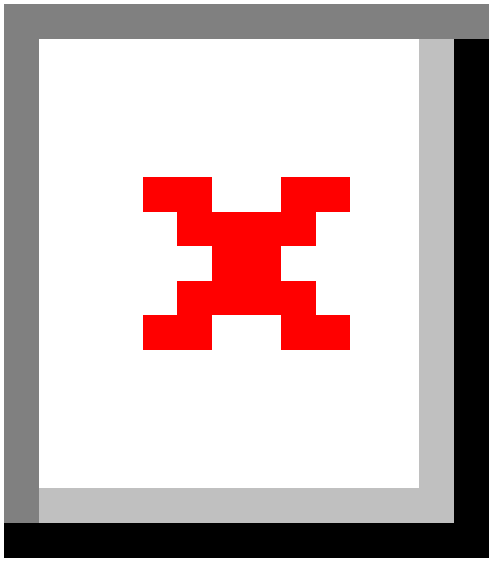
0x04 环境搭建

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

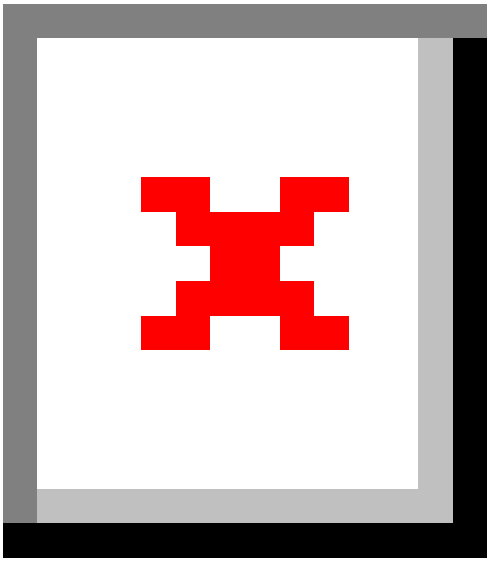




在pom.xml中，添加XStream依赖：

```
    <!--
https://mvnrepository.com/artifact/com.thoughtworks.xstream/xstr
eam -->
    <dependencies>
        <dependency>
            <groupId>com.thoughtworks.xstream</groupId>
            <artifactId>xstream</artifactId>
```

```
        <version>1.4.14</version>
    </dependency>
</dependencies>
```



到这里，我们在新建的XStream项目中引入了XStream依赖

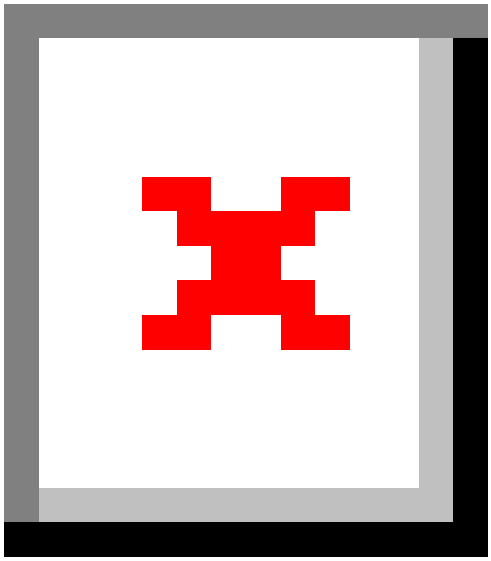
简单使用

新建一个Test.java文件，内容如下：

```
import com.thoughtworks.xstream.XStream;
import com.thoughtworks.xstream.io.json.JettisonMappedXmlDriver;

class Person//JavaBean实体类
{
    private String name;
    private int age;
    public Person(String name,int age)
    {
        this.name=name;
        this.age=age;
    }
    @Override
    public String toString()
    {
        return "Person [name=" + name + ", age=" + age + "]";
    }

}

public class Test
{
    public static void main(String[] args)
    {
```

```
        Person bean=new Person("美女",18);
        XStream xstream = new XStream();
        //XML序列化
        String xml = xstream.toXML(bean);
         System.out.println(xml);
        //        //XML反序列化
        bean=(Person)xstream.fromXML(xml);
        System.out.println(bean);

    }
}
```

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

https://github.com/jas502n/CVE-2020-26259/blob/main/CVE_2020_26258.java

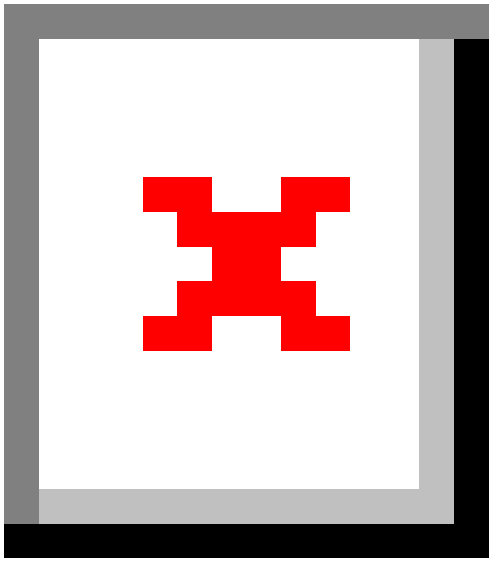
本地nc监听8989端口

CVE-2020-26259　任意文件删除

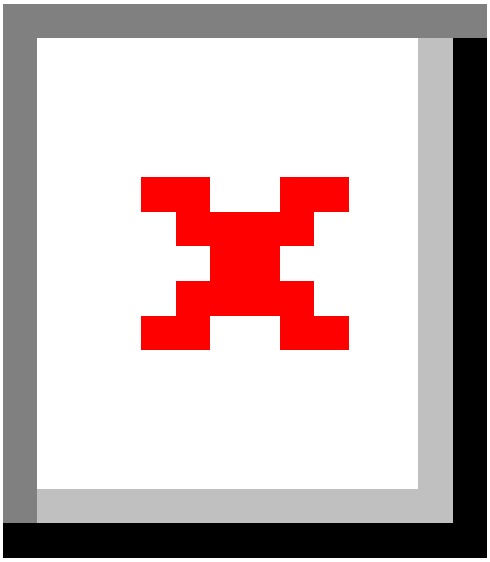
在main -> java下创建一个CVE-2020-26259.java文件，代码为

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

精选留言

用户设置不下载评论
阅读全文