安全漏洞通告

CVE-2020-26258/26259: XStream 反序列化漏洞通告

360CERT
北京奇虎科技有限公司 | 2020-12-14

报告信息

报告名称	CVE-2020-26258/26259: XStream 反序列化漏洞通告		
报告类型	安全漏洞通告	**报告编号**	B6-2020-121401
报告版本	1	**报告日期**	2020-12-14
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	2020-12-14	360CERT	360CERT	撰写报告

目录

一、 漏洞档案

漏洞类型	序列化漏洞
CVE 编号	CVE-2020-26259 等
相关厂商	XStream
相关组件	XStream 等
威胁等级	高危
影响面	广泛
360CERT 评分	8.9
修复方案	通用修补方案/临时修补方案
漏洞发布时间	2020-12-14
报告生成时间	2020-12-14

二、 漏洞简述

2020 年 12 月 14 日，360CERT 监测发现 XStream 发布了 XStream 反序列化漏洞 的风险通告，漏洞编号为 CVE-2020-26259,CVE-2020-26258 ，漏洞等级：高危，漏洞评分：8.9。

在运行 XSteam 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 任意文件删除/服务端请求伪造 。

目前该漏洞的 POC 已经公开

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	高危
影响面	广泛
360CERT 评分	8.9

四、 漏洞详情

CVE-2020-26259: 任意文件删除漏洞

只要（运行 XStream 服务的）进程有足够的权限，那么当 XStream 在反序列化数据时，攻击者构造特定的 XML/JSON 请求，可以造成任意文件删除。

CVE-2020-26258: 服务端请求伪造漏洞

运行 XStream 的服务在反序列化数据时，攻击者构造特定的 XML/JSON 请求，可以造成服务端请求伪造。

五、 影响版本

产品名称	影响版本
XStream	<=1.4.14

六、 安全建议

(一) 通用修补方案

升级至 1.4.15 版本，下载链接为：

https://x-stream.github.io/changes.html#1.4.15

(二) 临时修补方案

低于 1.4.15 的不同版本用户可以按照以下代码设置黑名单：

- 使用 XStream 1.4.14 的用户，只需在 XStream 的设置代码中添加两行即可：

```
xstream.denyTypes(new String[]{ "jdk.nashorn.internal.objects.NativeString" });
xstream.denyTypesByRegExp(new String[]{ ".*\\.ReadAllStream\\$FileStream" });
```

- 使用 XStream 1.4.13 的用户，只需在 XStream 的设置代码中添加三行代码即可：

```
xstream.denyTypes(new String[]{ "javax.imageio.ImageIO$ContainsFilter",
"jdk.nashorn.internal.objects.NativeString" });
xstream.denyTypes(new Class[]{ java.lang.ProcessBuilder.class });
xstream.denyTypesByRegExp(new String[]{ ".*\\.ReadAllStream\\$FileStream" });
```

- 使用 XStream 1.4.7 到 1.4.12 的用户，需要设置多个黑名单：

```
xstream.denyTypes(new String[]{ "javax.imageio.ImageIO$ContainsFilter",
"jdk.nashorn.internal.objects.NativeString" });
```

```
xstream.denyTypes(new Class[]{ java.lang.ProcessBuilder.class,
java.beans.EventHandler.class, java.lang.ProcessBuilder.class, java.lang.Void.class,
void.class });
xstream.denyTypesByRegExp(new String[]{ ".*\\$LazyIterator",
"javax\\.crypto\\..*", ".*\\.ReadAllStream\\$FileStream" });
```

- 使用 XStream 1.4.6 或更低版本的用户可以注册自己的 Converter ， 以防止反序列化当前已知的有危害的 Java 类型。

```
xstream.registerConverter(new Converter() {
public boolean canConvert(Class type) {
}
public Object unmarshal(HierarchicalStreamReader reader,
UnmarshallingContext context) {
throw new ConversionException("Unsupported type due to security reasons.");
}
public void marshal(Object source, HierarchicalStreamWriter writer,
MarshallingContext context) {
throw new ConversionException("Unsupported type due to security reasons.");
}
}, XStream.PRIORITY_LOW);
```

七、 参考链接

1. CVE-2020-26258 官方漏洞通告

   http://x-stream.github.io/CVE-2020-26258.html

2. CVE-2020-26259 官方漏洞通告

   http://x-stream.github.io/CVE-2020-26259.html

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 ≤ 360CERT 评分 ≤ 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 ≤ 360CERT 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	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 a) 占用存储空间 b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
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	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
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