安全漏洞通告

2021-08: XStream 多个高危漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	2021-08: XStream 多个高危漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-082301
报告版本	1	报告日期	2021-08-23
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-08-23	360CERT	360CERT	撰写报告

目录

1 风险简述

2021 年 08 月 23 日，360CERT 监测发现 XStream官方 发布了 XStream 的风险通告，漏洞编号为 CVE-2021-39139,CVE-2021-39140,CVE-2021-39141,CVE-2021-39144,CVE-2021-39145,CVE-2021-39146,CVE-2021-39147,CVE-2021-39148,CVE-2021-39149,CVE-2021-39150,CVE-2021-39151,CVE-2021-39152,CVE-2021-39153,CVE-2021-39154 ，漏洞等级：严重，漏洞评分：9.8。目前该漏洞安全补丁已更新，漏洞细节已公开，POC（概念验证代码）已公开，在野利用未发现。

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。

2 相关组件

XStream是Java类库，用来将对象序列化成 XML/JSON 或反序列化为对象，不需要其它辅助类和映射文件，使得XML序列化不再繁琐。XStream 在很多中间件中以第三方依赖的形式引入，使用广泛。

3 风险状态

类别	状态
安全补丁	已公开
漏洞细节	已公开
poc	已公开
在野利用	未发现
相关安全事件	未发现

4 风险等级

评定方式	等级
威胁等级	严重
影响面	一般
攻击者价值	高
利用难度	低
360CERT 评分	9.8

5 风险详情

5.1 CVE-2021-39139: XStream 代码执行漏洞

CVE: CVE-2021-39139

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

5.2 CVE-2021-39140: XStream 拒绝服务漏洞

CVE: CVE-2021-39140

组件: xstream

漏洞类型: 拒绝服务

影响: 拒绝服务

简述: 该漏洞可能允许远程攻击者根据 CPU 类型或此类负载的并行执行在目标系统上分配 100% 的 CPU 时间，从而仅通过操纵处理过的输入流导致拒绝服务。

5.3 CVE-2021-39141: XStream 代码执行漏洞

CVE: CVE-2021-39141

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加

载的任意代码。

5.4 CVE-2021-39144: XStream 代码执行漏洞

CVE: CVE-2021-39144

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

5.5 CVE-2021-39145: XStream 代码执行漏洞

CVE: CVE-2021-39145

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

5.6 CVE-2021-39146: XStream 代码执行漏洞

CVE: CVE-2021-39146

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

5.7 CVE-2021-39147: XStream 代码执行漏洞

CVE: CVE-2021-39147
组件: xstream
漏洞类型: 代码执行
影响: 服务器接管
简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

5.8 CVE-2021-39148: XStream 代码执行漏洞

CVE: CVE-2021-39148
组件: xstream
漏洞类型: 代码执行
影响: 服务器接管
简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

5.9 CVE-2021-39149: XStream 代码执行漏洞

CVE: CVE-2021-39149
组件: xstream
漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

5.10 CVE-2021-39150: XStream 服务器端请求伪造漏洞

CVE: CVE-2021-39150

组件: xstream

漏洞类型: 服务器端请求伪造

影响: 服务器端请求伪造

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而导致服务端请求伪造。

5.11 CVE-2021-39151: XStream 代码执行漏洞

CVE: CVE-2021-39151

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

5.12 CVE-2021-39152: XStream 服务器端请求伪造漏洞

CVE: CVE-2021-39152

组件: xstream

漏洞类型: 服务器端请求伪造

影响: 服务器端请求伪造

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而导致服务端请求伪造。

5.13 CVE-2021-39153: XStream 代码执行漏洞

CVE: CVE-2021-39153

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上本地执行命令。

5.14 CVE-2021-39154: XStream 代码执行漏洞

CVE: CVE-2021-39154

组件: xstream

漏洞类型: 代码执行

影响: 服务器接管

简述: 攻击者可以操纵已处理的输入流并替换或注入对象，从而执行从远程服务器加载的任意代码。

6 影响版本

组件	影响版本	安全版本
xstream	<1.4.18	1.4.18

7 修复建议

7.1 通用修补建议

建议升级到最新版本，并按照官方提供的缓解措施进行修复：

XStream 官方通告

8 时间线

2021-08-22 XStream 官方发布通告

2021-08-23 360CERT 发布通告

9 参考链接

XStream 官方通告

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 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获取对应产品。

A.2 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.3 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。