# XStream 拒绝服务漏洞

# CVE-2022-41966


2022 年 12 月 29 日

# 一、漏洞概要

| | |
|---|---|
| 漏洞名称 | **XStream 拒绝服务漏洞(CVE-2022-41966)** |
| 发布时间 | **2022 年 12 月 29 日** |
| 组件名称 | **XStream** |
| 影响范围 | **XStream ≤ 1.4.19** |
| 漏洞类型 | 拒绝服务 |
| 利用条件 | 1、用户认证：不需要权限认证<br>2、前置条件：默认条件<br>3、触发方式：远程 |
| 综合评价 | <综合评定利用难度>：容易，无需认证即可利用<br><综合评定威胁等级>：高危，可导致拒绝服务 |
| 官方解决方案 | 已发布 |

# 二、漏洞分析

## 2.1 组件介绍

XStream 是一个 Java 类库，用来将对象序列化成 XML、JSON 或反序列化为对象。XStream 是自由软件，可以在 BSD 许可证的许可下分发。

## 2.2 漏洞描述

2022 年 12 月 29 日，深信服安全团队监测到一则 XStream 组件存在拒绝服务漏洞的信息，漏洞编号：CVE-2022-41966，漏洞威胁等级：高危。

该漏洞是由于 XStream 进行反序列化时，未对输入的数据进行有效的验证。攻击者通过控制传入的序列化数据注入恶意对象，导致 Xstream 在递归计算 hash 集时触发堆栈溢出，最终导致拒绝服务。

## 三、影响范围

XStream 是较为流行的高性能计算类库，在世界范围内应用十分广泛。可能受漏洞影响的资产广泛分布于世界各地，在国内主要应用于上海、北京、浙江、广东、山东等地区。

目前受影响的 XStream 版本：

XStream ≤ 1.4.19

# 四、解决方案

## 4.1 修复建议

### 1.官方修复建议

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

https://x-stream.github.io/download.html

## 4.2 深信服解决方案

### 1.安全监测

支持对 XStream 拒绝服务漏洞(CVE-2022-41966)的监测，可依据流量收集实时监控业务场景中的受影响资产情况，快速检查受影响范围，相关产品及服务如下：

【深信服安全感知管理平台 SIP】预计 2022 年 12 月 30 日发布检测方案。

【深信服安全托管服务 MSS】预计 2022 年 12 月 30 日发布检测方案。

【深信服安全检测与响应平台 XDR】预计 2022 年 12 月 30 日发布检测方案。

### 2.安全防护

支持对 XStream 拒绝服务漏洞(CVE-2022-41966)的防御，可阻断

**攻击者针对该事件的入侵行为**，相关产品及服务如下：

【深信服下一代防火墙 AF】预计 2022 年 12 月 30 日发布防护方案。

【深信服 Web 应用防火墙 WAF】预计 2022 年 12 月 30 日发布防护方案。

【深信服安全托管服务 MSS】预计 2022 年 12 月 30 日发布防护方案。

【深信服安全检测与响应平台 XDR】预计 2022 年 12 月 30 日发布防护方案。

## 五、时间轴

2022/12/29　深信服监测到 XStream 拒绝服务漏洞攻击信息。

2022/12/29　深信服千里目安全技术中心发布漏洞通告。

# 六、参考链接

https://x-stream.github.io/CVE-2022-41966.html

# 七、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。