

XStream 多个反序列化漏洞

一、漏洞信息

2021年8月23日, Xstream 发布了安全通告, 其中包含了 CVE-2021-39139, CVE-2021-39144, CVE-2021-39150 等多个反序列化漏洞的漏洞修复。

- **CVE-2021-39140**

当 XStream 在反序列化数据时, 攻击者构造特定的 XML 序列化数据, 将可能导致无限循环, 从而造成拒绝服务漏洞。

- **CVE-2021-39150/CVE-2021-39152**

当 XStream 在反序列化数据时, 攻击者构造特定的 XML 序列化数据, 将导致服务端请求伪造漏洞, 攻击者通过该漏洞可以访问内网资源。

- **CVE-2021-39139/CVE-2021-39141/CVE-2021-39144/CVE-2021-3**

9145/CVE-2021-39146/CVE-2021-39147/CVE-2021-39148/CVE-2

021-39149/CVE-2021-39151/CVE-2021-39153/CVE-2021-39154

当 XStream 在反序列化数据时, 攻击者构造特定的 XML 序列化数据, 将导致远程代码执行漏洞

二、漏洞危害

- **CVE-2021-39140**

当 XStream 在反序列化数据时, 攻击者构造特定的 XML 序列化数据, 将可能导致无限循环, 从而造成拒绝服务漏洞。

- **CVE-2021-39150/CVE-2021-39152**

当 XStream 在反序列化数据时, 攻击者构造特定的 XML 序列化数据, 将导致服务端请求伪造漏洞, 攻击者通过该漏洞可以访问内网资源。

- **CVE-2021-39139/CVE-2021-39141/CVE-2021-39144/CVE-2021-3**

9145/CVE-2021-39146/CVE-2021-39147/CVE-2021-39148/CVE-2

021-39149/CVE-2021-39151/CVE-2021-39153/CVE-2021-39154

