关于XStream 多个高危漏洞风险提示（CVE-2021-39140、CVE-2021-39144、CVE-2021-39139、CVE-2021-39141、CVE-2021-39145、CVE-2021-39146、CVE-2021-39147、CVE-2021-39148、CVE-2021-39149、CVE-2021-39151、CVE-2021-39153、CVE-2021-39154、CVE-2021-39150、CVE-2021-39152 CVE-2021-39139）

漏洞相关 吴昊A 2021-08-26 发表

漏洞相关信息

漏洞编号： CVE-2021-39140、CVE-2021-39144、CVE-2021-39139、CVE-2021-39141、CVE-2021-39145、CVE-2021-39146、CVE-2021-39147、CVE-2021-39148、CVE-2021-39149、CVE-2021-39151、CVE-2021-39153、CVE-2021-39154、CVE-2021-39150、CVE-2021-39152 CVE-2021-39139

漏洞名称： XStream 多个高危漏洞

产品型号及版本： V7防火墙 SSM-G2 SecPath A2020-G CSAP-SA-V

漏洞描述

一、背景介绍

8月23日，市委网信办技术支撑单位监测到XStream官方发布安全公告，公开了XStream 中的14 个安全漏洞（CVE-2021-39140、CVE-2021-39144、CVE-2021-39139、CVE-2021-39141、CVE-2021-39145、CVE-2021-39146、CVE-2021-39147、CVE-2021-39148、CVE-2021-39149、CVE-2021-39151、CVE-2021-39153、CVE-2021-39154、CVE-2021-39150、CVE-2021-39152）。

1.1 漏洞描述

CVE-2021-39140

攻击者可以操纵已处理的输入流并替换或注入对象，这会导致一个无休止的循环，从而造成拒绝服务攻击。

CVE-2021-39144

攻击者可以操作已处理的输入流并替换或注入对象，从而在服务器上远程执行命令。

CVE-2021-39139、CVE-2021-39141、CVE-2021-39145、CVE-2021-39146、CVE-2021-39147、CVE-2021-39148、CVE-2021-39149、CVE-2021-39151、CVE-2021-39153、CVE-2021-39154

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。

CVE-2021-39150、CVE-2021-39152

攻击者可以操纵已处理的输入流并替换或注入对象，从而实现服务端请求伪造。

1.2漏洞编号

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

1.3风险等级

高危

二、修复建议

漏洞解决方案

不涉及

2.1受影响版本

XStream <= 1.4.17

2.2修复建议

目前官方已在最新版本中采用白名单的方式修复了以上漏洞，请受影响的用户尽快升级版本进行防护。

官方下载链接：https://x-stream.github.io/download.html