Closed Opened 1 week ago by muffinx

XML External Entity Attacks

Dear E-Voting PIT Team

Glad to get in touch with you again, even though we try to not spam you.

Here we provide you with potential XXE vulnerabilites. (We checked for all the common java xml parsing classes)

TransformerFactory

/evoting-solution/source-code/scytl-cryptolib/cryptolib-asymmetric/src/main/java/com/scytl/cryptolib/asymmetric/utils/DomUtils.java

```
// Write DOM data to output stream.
try {
    TransformerFactory transformerFactory =
        TransformerFactory.newInstance();
    transformerFactory.setAttribute(
        XMLConstants.ACCESS_EXTERNAL_DTD, "");

    Transformer transformer = transformerFactory.newTransformer();
    transformer.setOutputProperty(OutputKeys.OMIT_XML_DECLARATION,
        "yes");
    transformer.transform(new DOMSource(dom), new StreamResult(
        outStream));
} catch (TransformerException e) {
    throw new GeneralSecurityException(
        DOM_DATA_WRITE_ERROR_MESSAGE, e);
} finally {
    closeQuietly(outStream);
}
```

There is an important setting missing:

```
transformerFactory.setAttribute(XMLConstants.ACCESS_EXTERNAL_STYLESHEET, "");
```

JAXB Unmarshaller

We are not sure about this one.

/home/muffinx/projects/evoting-solution/source-code/online-voting-secure-data-manager/secure-data-manager-backend/secure-data-manager-integration/src/main/java/com/scytl/products/ov/sdm/plugin/XmlObjectsLoader.java

```
private static Unmarshaller create(String schemaPath, Class<?> clazz) throws JAXBException, SAXException {
    Unmarshaller unmarshaller = JAXBContext.newInstance(clazz).createUnmarshaller();
    if (schemaPath != null) {
        Schema schema = getSchema(schemaPath, clazz);
        unmarshaller.setSchema(schema);
    }
    return unmarshaller;
}
```

Now there is a schema being set with anti-XXE settings, but still we are not sure about the effectiveness of this approach (pretty specific question):

```
public static Plugins unmarshal(Path xml) throws IOException, JAXBException, SAXException {
      return unmarshal(xml, "/xsd/plugins.xsd", Plugins.class);
  }

  @SuppressWarnings("unchecked")
  public static <T> T unmarshal(final Path xml, final String schemaPath, Class<?> clazz)
      throws IOException, JAXBException, SAXException {
```

```
    try (InputStream is = Files.newInputStream(xml)) {
        return (T) create(schemaPath, clazz).unmarshal(is);
    }
}

private static Unmarshaller create(String schemaPath, Class<?> clazz) throws JAXBException, SAXException {
    Unmarshaller unmarshaller = JAXBContext.newInstance(clazz).createUnmarshaller();
    if (schemaPath != null) {
        Schema schema = getSchema(schemaPath, clazz);
        unmarshaller.setSchema(schema);
    }
    return unmarshaller;
}
```

We include this to be 100% sure.

SAXReader

\evoting-solution-master\source-code\maven-generic-conf\extlibs\ec2-plugin\src\main\java\hudson\plugins\ec2\Eucalyptus.java

```
try {
                HttpsURLConnection con = (HttpsURLConnection)metadataUrl.openConnection();
                makeIgnoreCertificate(con);
                Document metadata = new SAXReader().read(con.getInputStream());
                this.ec2endpoint = readURLFromMetadata(metadata, "ec2");
                this.s3endpoint = readURLFromMetadata(metadata, "s3");
           }
```

The class is directly initialized with missing settings:

```
SAXBuilder builder = new SAXBuilder();
builder.setFeature("http://apache.org/xml/features/disallow-doctype-decl",true);
builder.setFeature("http://xml.org/sax/features/external-general-entities", false);
builder.setFeature("http://xml.org/sax/features/external-parameter-entities", false);
Document doc = builder.build(new File(fileName));
```

Take these serious as well, since if these work, an attacker could leak files and do SSRF attacks.

Thank you very much for reading our report.

Best Regards

Anthony Schneiter aka. muffinx Jannis Kirschner aka. xorkiwi

Swisspost @swisspost added In Progress topic: general labels 1 week ago

Swisspost @swisspost · 1 week ago Maintainer

Hello,

Thank your for your input. We will verify this and get back to you.

Kind regards

Swisspost @swisspost · 3 days ago Maintainer

Hello Anthony,

Thank you for your observation. It is indeed a bug in the DomUtils.java class. We are going to fix it in a future version. Since this class is not used in the sVote solution (sVote does not work with XML for Cryptolib related operations), we consider it a minor bug.

Does this reply suffice to you?

Kind regards

Swisspost @swisspost closed 3 days ago

Swisspost @swisspost removed In Progress label 1 day ago

Swisspost @swisspost made the issue visible to everyone 1 day ago