New issue

Jump to bottom

XXE in apikit #547

Closed **prodigysml** opened this issue on Mar 25, 2020 · 1 comment

prodigysml commented on Mar 25, 2020

While reading the code in the apikit project we (**@n33dle** and I) identified a vulnerability we wanted to raise. The vulnerability is an XXE vulnerability (https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing) and can be identified in the lines of code below:

apikit/mule-module-apikit/src/main/java/org/mule/module/apikit/validation/RestXmlSchemaValidator.java
Lines 150 to 158 in 8b38394

```
150     DocumentBuilderFactory factory = DocumentBuilderFactory.newInstance();
151     setFeatures(factory);
152     factory.setNamespaceAware(true);
153     try
154     {
155         DocumentBuilder builder = factory.newDocumentBuilder();
156         //Setting error handler to null to avoid logs generated by the parser.
157         builder.setErrorHandler(null);
158         return builder.parse(source);
```

juanchib commented on Jul 17, 2020 Contributor

The attack is prevented at setFeatures() method, tests for this are found at org.mule.module.apikit.schema.XxeAttackTestCase , thanks for the adivse.

juanchib closed this as completed on Jul 17, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants