Jadx-gui: Swing HTML DOS attack

Moderate skylot published GHSA-3r7j-8mqh-6qhx on Oct 20

Package

jadx-gui (binary release)

Affected versions	Patched versions
<= 1.4.4	1.4.5

Description

Impact

Using jadx-gui to open a special zip file with entry containing HTML sequence like `<html><frame>` will cause interface to get stuck and throw exceptions like:

```
java.lang.RuntimeException: Can't build aframeset, BranchElement(frameset) 1,3
:no ROWS or COLS defined.
        at
java.desktop/javax.swing.text.html.HTMLEditorKit$HTMLFactory.create(HTMLEditorKit.java:1387)
        at
java.desktop/javax.swing.plaf.basic.BasicHTML$BasicHTMLViewFactory.create(BasicHTML.java:379)
        at java.desktop/javax.swing.text.CompositeView.loadChildren(CompositeView.java:112)
```

References

https://www.oracle.com/java/technologies/javase/seccodeguide.html

Guideline 3-7 / INJECT-7: Disable HTML display in Swing components:

Many Swing pluggable look-and-feels interpret text in certain components starting with as HTML. If the text is from an untrusted source, an adversary may craft the HTML such that other components appear to be present or to perform inclusion attacks.

To disable the HTML render feature, set the "html.disable" client property of each component to Boolean.TRUE (no other Boolean true instance will do).

```
    label.putClientProperty("html.disable", true);
```

Severity

Moderate

CVE ID

CVE-2022-39259

Weaknesses

CWE-75