Vulnerability: Arbitrary JSP C AdminDesignAction Leads tc Execution in Fess ≤ 15.5.1

BUG_Author: R1ckyZ

Affected Version: Fess ≤ 15.5.1

Vendor: CodeLibs

Software: Fess

Vulnerability Files:

- `org/codelibs/fess/app/web/admin/design/Adm`

Description:

The `update()` method in `AdminDesignAction` writes u after passing it through `decodeJsp()`. The filter only escap tags — JSP EL expressions (`${}`) are not touched at all:

Code block

```
1  // AdminDesignAction.java:284
2  write(jspFile.getAbsolutePath(), decodeJsp(f
3
4  // AdminDesignAction.java:405-407
5  public static String decodeJsp(String value)
6      return value
7          .replaceAll("<%(?![@-])([\\s\\S]*?)%
8          .replaceAll("<%=([\\s\\S]*?)%>", "&l
9          // ${ } EL expressions: NOT filtered
10         .replace(TRY_STATEMENT, "<% try{ %>"
11         .replace(CACHE_AND_SESS _INVALIDATI
12 }
```