

OfBiz

CVE-2017-15714

Context

It occurs in the BIRT plug-in, in the code that is used to Map Java attributes to Javascript constants.

Problem

The BIRT plugin in Apache OFBiz does not escape user input property passed. This allows for code injection by passing that code through the URL. For example by appending this code "__format=%27;alert(%27xss%27)" to the URL an alert window would execute.

Solution

Fix is to enforce html encoding of request-strings passed to birt. This is done by invoking (which escapes HTML characters)

```
htmlEncode(ParameterAccessor.getFormat(request))
```

Issue Tracking URL

-

Commit URL

- <https://svn.apache.org/viewvc?view=revision&revision=1818482>