

New issue

Jump to bottom

XSS in the file upload functionality #32

Open uzakov opened this issue on Feb 12, 2020 · 9 comments

uzakov commented on Feb 12, 2020

There is an XSS(Cross-site scripting) present in the file upload functionality, where someone can upload a file with malicious filename, which contains JavaScript code, which would results in XSS. Example: <https://github.com/manolo/gwtupload/blob/master/samples/src/main/java/gwtuploadsample/client/SingleUploadSample.java>

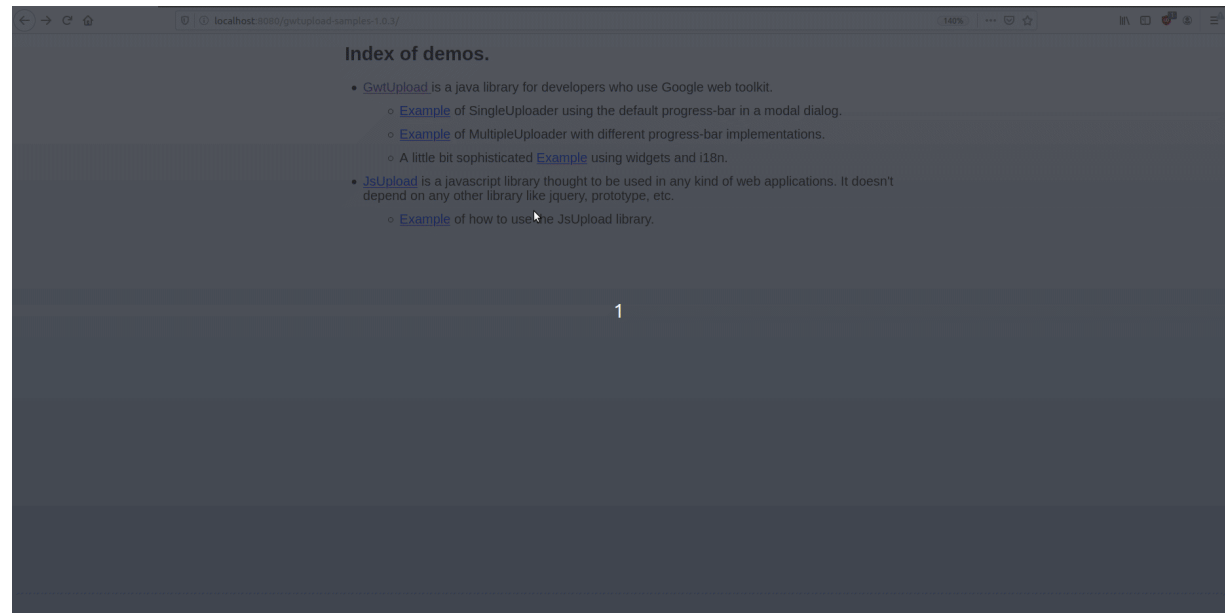


How to reproduce:

1. Deploy SingleUploadSample war file (<https://mvnrepository.com/artifact/com.googlecode.gwtupload/gwtupload-samples/1.0.3>)
2. Upload a file from a Linux system(due to Windows filename character restrictions), which contains JavaScript code. For example: a ``

uzakov commented on Mar 2, 2020

Author



stumoss added a commit to stumoss/gwtupload that referenced this issue on Mar 4, 2020

Fix issue [mano1o#32](#). ...

9164fd4

stumoss added a commit to clearswift/gwtupload that referenced this issue on Mar 4, 2020

Fix issue [mano1o#32](#). ...

eca56a0

sankosk commented on Oct 2, 2020

that's a self-XSS, exploitability is almost null.



uzakov commented on Oct 2, 2020

Author

@sankosk Would have to disagree on the "exploitability is almost null". Many OS and applications do not show full filename, only showing first X characters. User would not see the JS code at the end of the filename in many scenarios.

sankosk commented on Oct 2, 2020

@uzakov I agree that's a bad practice and there are multiple scenarios where it can be useful.
However, official score you've set for the CVE is 6,4, which is extremely high and for sure not even close to reality. Proper scoring should be lower, rounding 3-4.

  csware mentioned this issue on Feb 14, 2021

CVE-2020-9447 #34

 Open

csware commented on Feb 14, 2021

Contributor

cf. PR [#36](#)

Roleek commented on Mar 10, 2021

Pen testers identified this as an issue in our application and refused to accept reasoning that this is actually affects only the one who uploads the file. So here is my patch that fixes the issue. The idea of the patch is not to send file name back to client side to avoid JavaScript in file name to be executed as part of alert on client side.
[0001-Fixes-that-uploading-a-file-with-malicious-filename-.zip](#)

akash-chourasia commented on Dec 21, 2021

Hi,

Is there any chance that new version will be released with the Vulnerability fixes.

SSK-code commented on Mar 21

Is there any update on this issue.
I am facing the XSS due to file name.

raghulvishnudhin... commented on Jun 15

Please let me know the workaround or the solution for this fix

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

7 participants

