

Forum:[Hack Forums](#)

Thread: [LifeRay CMS \(Fckeditor\) Arbitrary File Upload Vulnerability](#)

OfficeInboxer - April 26, 2020, 2:52 pm

- [+] Title: LifeRay File Upload (CKEditor Vulnerable)
- [+] Date: 2020-04-20
- [+] Vendor Homepage: www.liferay.com
- [+] Software Link: www.liferay.com
- [+] Tested on: Windows 10 &&&& Google Chrome
- [+] Version : All Versions
- [+] Category : Web Application Bugs
- [+] Vulnerable File: /browser.html
- [+] Dork : inurl:/ckeditor/editor/filemanager/

POC:

[+] Exploit : site.com/html/js/editor/ckeditor/editor/filemanager/browser/liferay/browser.html

Note:

If you are careful, in the exploit that friends find, it is in the folder (FCKEditor) and the exploit that I found is in the folder (CKEditor).

This exploit has been tested in all versions of LifeRay and the file can be uploaded in all tested sites.

Exploits found by friends (note the folder &&&"FCKEditor&&&"):
/html/js/editor/fckeditor/editor/filemanager/browser/liferay/browser.html Newly discovered exploits
(see folder &&&"CKEditor&&&"):
/html/js/editor/ckeditor/editor/filemanager/browser/liferay/browser.html

LifeRay allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. Uploaded files represent a significant risk to applications.

m0dvi3w - April 27, 2020, 6:50 pm

This vuln is old AF, but is still out there. Also there is way more you can do than just that POC ;)

frank3nstien - April 27, 2020, 9:48 pm

This is really old mate, why don't you check history before ?

goratberom - March 28, 2021, 5:23 am

indeed old but if it is valid