Packages - Freedom Issue #2131

[metasploit] confirmed non-free

2019-01-06 07:40 AM - Anonymous

Status:	not-a-bug	**% Done:**	0%
Priority:	freedom issue		
Assignee:			
Category:			

Description
In 2017, I said that Metasploit might be non-free. Now I have found some Ruby gems, license for which is unknown (https://github.com/rapid7/metasploit-framework/blob/master/LICENSE_GEMS). Issue #1441 is no longer updated, even after my comment, so I think it is abandoned.
Related issues:
Related to Packages - Freedom Issue #1441: [metasploit] is not fully free   **not-a-bug**

History

#1 - 2019-01-06 12:49 PM - bill-auger

- Priority changed from bug to freedom issue

- Status changed from open to info needed

duplicate of #1441

#2 - 2019-01-06 12:49 PM - bill-auger

it does not help anything to have multiple open issues for the identical concern - you could as well have added to the original, and it would have floated to the top just the same as this one

this seems to about a ruby gem - yes? - that could explain why it was not given much attention - parabola does not support or filter software from third-party package managers - these are considered essentially the same as the AUR (this is: not recommended nor supported) - use at your own risk

is this regarding a package in the parabola repos ?

#3 - 2019-01-06 12:50 PM - bill-auger

- Related to Freedom Issue #1441: [metasploit] is not fully free added

#4 - 2019-01-07 12:48 PM - Anonymous

Yes, it looks like this gem is required by metasploit package.
Also, Metasploit recommends non-free software Metasploit Pro at every run.

#5 - 2019-01-07 10:52 PM - Anonymous

Update: all gems with "unknown" license are free, license is not found by the script for some reason.
Metasploit Pro is recommended at start but user must follow the link to get it.

#6 - 2022-01-20 11:56 PM - gap

metasploit was never blacklisted.

#7 - 2022-01-21 12:09 AM - gap

I believe the files of nonfree formats are crafted in order to allow exploits to be used for penetration testing.

Should we allow nonfree file formats if they're not being recommended for general-purpose use, but instead being used as proof-of-concept data specifically for pen testing?
They're still nonfree, and many of the formats are probably patented, so I'd err on the side of removal, although this would cause a massive issue for pen testers.

#8 - 2022-01-21 12:24 AM - bill-auger

according to this ticket comments, the package was not blacklisted
(yet), due to lack of evidence - that is why the 'Status' is still

'info-needed' - if it is decided, that it should be blacklisted,
the 'Status' would be 'confirmed', 'in-progress', then eventually
'fixed' - if it is decided, that it should not be blacklisted,
the 'Status' would be 'wont-fix' or 'not-a-bug'

note, the final comment (from the OP), when this ticket was fresh:

> Update: all gems with "unknown" license are free, license is not
> found by the script for some reason. Metasploit Pro is
> recommended at start but user must follow the link to get it.

so, if that is all true, then it is 100% free software (no
freedom concerns) - the problem remaining, is perhaps only the
advertisement for the non-free version (an FSDG concern)

put another way, the OP probably would not have opened this ticket,
if not for the missing license declarations - the OP clearly had no
further interest after it was discovered (by the same person) to be
libre - if the ticket had been closed on that day 'not-a-bug', it
would probably not be a topic of discussion today

what is most unfortunate, is that the OP did not state which licenses
those "unknown" packages actually do have; but abandoned the discussion
before anything tangible was concluded - so this ticket is basically at
square-1 (as if it were opened only today) - almost nothing is actually
known about its FSDG status (other than the words of "Anonymous", who is
obviously no longer interested in a resolution)

gap - FWIW, it is good that you noticed it - i am not complaining about
that - it would be great to close some of these old tickets - im only
explaining why nothing was done yet - it's not yet clear that there is
any problem(s) to address

#9 - 2022-01-21 12:48 AM - gap

One can view the metasploit package file list and observe **tons** of files of proprietary formats, eg. .doc, .swf, etc.
Moreover, none of these files are licensed clearly, so I must conclude they are unlicensed and as such are proprietary.

Also, since it's been so long, the advert might have been removed, and I don't want to install tons of proprietary files to my system to find out.

Thank you, Bill (if I'm okay to call you by your first name).
I have thick skin; I'm not easily offended and I understand we're all here working for a common goal.

#10 - 2022-01-21 01:03 AM - bill-auger

> Should we allow nonfree file formats

file formats are not a problem inherently - the software needed to decode/encode some file may be non-free, and parabola would not provide it; but the work itself could be distributed by parabola, if it is not an essential part of the program (demos/examples, documentation, etc)

i do not suppose that a file format would make any file non-free - most likely, one would need a non-free program to read or edit it; but the file may afford all four freedoms - what is most significant, is whether or not the "work" embodied by the file is freely licensed

#11 - 2022-01-21 01:07 AM - bill-auger

> I have thick skin; I'm not easily offended and I understand we're all here working for a common goal.

excellent - that, along with long-term dedication, are the only essential qualifications for the much needed "Parabola Community Team Leader" job - i thusly nominate you - congrats :)

#12 - 2022-01-21 01:24 AM - gap

It's worth noting that setting an issue to "not-a-bug" means it's no longer classed as "open", so it's easy for unconfirmed issues to get buried.

Edit: I mistook "not-a-bug" for "info-needed"; the former are classed as "closed", whilst the latter are classed as "open".
I mistakenly thought that "info-needed" issues were classed as "closed".

#13 - 2022-01-21 01:26 AM - gap

Thank you, Bill.
I have some more ideas to share on the forum, soon.

#14 - 2022-01-21 06:56 AM - bill-auger

'not-a-bug' and 'unconfirmed' are mutually exclusive states

'unconfirmed' and 'info-needed' tickets would be buried only over
time by newer tickets - if the alleged problem is demonstrated
reproducibly, it would go into the 'confirmed' or state

'not-a-bug' and 'wont-fix' tickets have no priority - they exist
for historical documentation purposes - they can be (should be)
buried/hidden WRT the "recent issues" list - they will not be
lost - redmine's search box can find them, usually by package
name

#15 - 2022-08-27 05:28 PM - GNUtoo

Anonymous wrote:

> Update: all gems with "unknown" license are free, license is not found by the script for some reason.
> Metasploit Pro is recommended at start but user must follow the link to get it.

Where does that (did?) take place?

With the current version, I didn't see advertisements:


```
$ msfconsole

     .:okOOOkdc'              'cdkOOOko:.
   .xOOOOOOOOOOOOc          cOOOOOOOOOOOOx.
  :OOOOOOOOOOOOOOOk,     ,kOOOOOOOOOOOOOOOO:
 'OOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOOOO'
 oOOOOOOOO.MMMM.oOOOoOOOOl.MMMM,OOOOOOOOo
 dOOOOOOOO.MMMMMM.cOOOOc.MMMMMM,OOOOOOOOx
 lOOOOOOOO.MMMMMMMM;d;MMMMMMMM,OOOOOOOOl
 .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
  cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
   oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
    lOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOl
     ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
      .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
        ,kOl'M.OOOOOOOOOOOOOO.M'dOk,
          :kk;.OOOOOOOOOOOO.;Ok:
            ;kOOOOOOOOOOOOOOk:
              ,xOOOOOOOOOOOx,
                .lOOOOOOOl.
                  ,dOd,
                    .

       =[ metasploit v6.2.13-dev                    ]
+ -- --=[ 2239 exploits - 1181 auxiliary - 398 post      ]
+ -- --=[ 864 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 >
```

With msfvenom, we don't have advertisement either:


```
$ msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /opt/metasploit/msfvenom [options] <var=val>
Example: /opt/metasploit/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: payloads, encoders, nops, platfor
```

```
ms, archs, encrypt, formats, all
    -p, --payload          <payload>  Payload to use (--list payloads to list, --list-options for arguments). S
pecify '-' or STDIN for custom
        --list-options                List --payload <value>'s standard, advanced and evasion options
    -f, --format           <format>   Output format (use --list formats to list)
    -e, --encoder          <encoder>  The encoder to use (use --list encoders to list)
        --service-name     <value>    The service name to use when generating a service binary
        --sec-name         <value>    The new section name to use when generating large Windows binaries. Defau
lt: random 4-character alpha string
        --smallest                    Generate the smallest possible payload using all available encoders
        --encrypt          <value>    The type of encryption or encoding to apply to the shellcode (use --list
encrypt to list)
        --encrypt-key      <value>    A key to be used for --encrypt
        --encrypt-iv       <value>    An initialization vector for --encrypt
    -a, --arch             <arch>     The architecture to use for --payload and --encoders (use --list archs to
 list)
        --platform         <platform> The platform for --payload (use --list platforms to list)
    -o, --out              <path>     Save the payload to a file
    -b, --bad-chars        <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled          <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                    Use nopsled size specified by -n <length> as the total payload size, auto
-prepending a nopsled of quantity (nops minus payload length)
    -s, --space            <length>   The maximum size of the resulting payload
        --encoder-space    <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations       <count>    The number of times to encode the payload
    -c, --add-code         <path>     Specify an additional win32 shellcode file to include
    -x, --template         <path>     Specify a custom executable file to use as a template
    -k, --keep                        Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name         <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout          <second>   The number of seconds to wait when reading the payload from STDIN (defaul
t 30, 0 to disable)
    -h, --help                        Show this message
```

As I understand, the advertisement was the last issue, so if there is no more advertisement, we could close this bug (we have between 100 and 200 freedom bugs open and between 700 and 800 bugs total just for the packages).

edit1: Added last sentence

#16 - 2022-12-13 02:55 PM - GNUtoo

- Status changed from info needed to not-a-bug

As we have between 700 and 800 bugs open, for now I'll close this bug as not-a-bug in order to not have too much bugs waiting for input that can never come. Feel free to reopen the bug if you have additional information so we could continue working on it.