New issue

Jump to bottom

code execution backdoor #4

Closed di1l0o opened this issue on Jun 13 · 1 comment

di1l0o commented on Jun 13

We found a malicious backdoor in versions 0.2.0b0~0.2.6.0b0 of this project, and its malicious backdoor is the request package. Even if the request package was removed by pypi, many mirror sites did not completely delete this package, so it could still be installed.When using pip install dr-web-engine==0.2.6.0b0 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install dr-web-engine==0.2.6.0b0 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting dr-web-engine==0.2.6.0b0
  Downloading http://pypi.doubanio.com/packages/3b/d7/5f291d203208779621 0f08262471d4cf02b71ae129985bb0ca29d7f67bdc/dr_web_engine-0.2.6.0b0-py3-none-any.whl (24 kB)
Collecting geckodriver-autoinstaller
  Downloading http://pypi.doubanio.com/packages/99/a0/527dd9b38cbb198e12ac1878a51cd86136222ffc1d131039e6286a6b57dc/geckodriver_autoinstaller-0.1.0-py3-none-any.whl (5.6 kB)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: selenium in /usr/local/lib/python3.8/dist-packages (from dr-web-engine==0.2.6.0b0) (4.1.5)
Requirement already satisfied: lxml in /usr/local/lib/python3.8/dist-packages (from dr-web-engine==0.2.6.0b0) (4.8.0)
Collecting python-interface
  Downloading http://pypi.doubanio.com/packages/fc/e9/092908ad6587b2537ab19fd68cea2eae520321530f23c4b82af71a38b8a1/python-interface-1.6.1.tar.gz (19 kB)
Collecting argparse
  Downloading http://pypi.doubanio.com/packages/f2/94/3af39d34be01a24a6e65433d19e107099374224905f1e0cc6bbe1fd22a2f/argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Collecting xvfbwrapper
  Downloading http://pypi.doubanio.com/packages/57/b6/4920eabda9b49630dea58745e79f9919aba6408d460afe758bf6e9b21a04/xvfbwrapper-0.2.9.tar.gz (5.6 kB)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->dr-web-engine==0.2.6.0b0) (2.27.1)
Requirement already satisfied: trio~=0.17 in /usr/local/lib/python3.8/dist-packages (from selenium->dr-web-engine==0.2.6.0b0) (0.20.0)
Requirement already satisfied: trio-websocket~=0.9 in /usr/local/lib/python3.8/dist-packages (from selenium->dr-web-engine==0.2.6.0b0) (0.9.2)
Requirement already satisfied: urllib3[secure,socks]~=1.26 in /usr/local/lib/python3.8/dist-packages (from selenium->dr-web-engine==0.2.6.0b0) (1.26.9)
Requirement already satisfied: six in /usr/local/lib/python3.8/dist-packages (from python-interface->dr-web-engine==0.2.6.0b0) (1.16.0)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->dr-web-engine==0.2.6.0b0) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->dr-web-engine==0.2.6.0b0) (2021.10.8)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->dr-web-engine==0.2.6.0b0) (2.0.12)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from trio~=0.17->selenium->dr-web-engine==0.2.6.0b0) (21.4.0)
Requirement already satisfied: sortedcontainers in /usr/local/lib/python3.8/dist-packages (from trio~=0.17->selenium->dr-web-engine==0.2.6.0b0) (2.4.0)
Requirement already satisfied: outcome in /usr/local/lib/python3.8/dist-packages (from trio~=0.17->selenium->dr-web-engine==0.2.6.0b0) (1.1.0)
Requirement already satisfied: sniffio in /usr/local/lib/python3.8/dist-packages (from trio~=0.17->selenium->dr-web-engine==0.2.6.0b0) (1.2.0)
Requirement already satisfied: async-generator>=1.9 in /usr/local/lib/python3.8/dist-packages (from trio~=0.17->selenium->dr-web-engine==0.2.6.0b0) (1.10)
Requirement already satisfied: wsproto>=0.14 in /usr/local/lib/python3.8/dist-packages (from trio-websocket~=0.9->selenium->dr-web-engine==0.2.6.0b0) (1.1.0)
Requirement already satisfied: cryptography>=1.3.4; extra == "secure" in /usr/local/lib/python3.8/dist-packages (from urllib3[secure,socks]~=1.26->selenium->dr-web-engine==0.2.6.0b0) (36.0.
2)
Requirement already satisfied: pyOpenSSL>=0.14; extra == "secure" in /usr/local/lib/python3.8/dist-packages (from urllib3[secure,socks]~=1.26->selenium->dr-web-engine==0.2.6.0b0) (22.0.0)
Requirement already satisfied: PySocks!=1.5.7,<2.0,>=1.5.6; extra == "socks" in /usr/local/lib/python3.8/dist-packages (from urllib3[secure,socks]~=1.26->selenium->dr-web-engine==0.2.6.0b0)
 (1.7.1)
Requirement already satisfied: h11<1,>=0.9.0 in /usr/local/lib/python3.8/dist-packages (from wsproto>=0.14->trio-websocket~=0.9->selenium->dr-web-engine==0.2.6.0b0) (0.13.0)
Requirement already satisfied: cffi>=1.12 in /usr/local/lib/python3.8/dist-packages (from cryptography>=1.3.4; extra == "secure"->urllib3[secure,socks]~=1.26->selenium->dr-web-engine==0.2.6
.0b0) (1.15.0)
Requirement already satisfied: pycparser in /usr/local/lib/python3.8/dist-packages (from cffi>=1.12->cryptography>=1.3.4; extra == "secure"->urllib3[secure,socks]~=1.26->selenium->dr-web-en
gine==0.2.6.0b0) (2.21)
Building wheels for collected packages: python-interface, xvfbwrapper
  Building wheel for python-interface (setup.py) ... done
  Created wheel for python-interface: filename=python_interface-1.6.1-py3-none-any.whl size=23224 sha256=8ce9c0dff2b62d439c96c8247510667f03ebf73852dfcde570dbfa811df330f8
  Stored in directory: /root/.cache/pip/wheels/f7/3b/94/27bfcd2906a2be057c16f1f23273bb28bcbc4dbc6a3d3f14fb
  Building wheel for xvfbwrapper (setup.py) ... done
  Created wheel for xvfbwrapper: filename=xvfbwrapper-0.2.9-py3-none-any.whl size=5008 sha256=58a7a2fa596cd7eb96f911c246464ff852f27fe96ad1ff9ca26a8aeb26e7c432
  Stored in directory: /root/.cache/pip/wheels/5a/33/48/e350e5302b94ea2dc35f94a0c12ba9f6de5a0e711d629d3a75
Successfully built python-interface xvfbwrapper
Installing collected packages: geckodriver-autoinstaller, request, python-interface, argparse, xvfbwrapper, dr-web-engine
Successfully installed argparse-1.4.0 dr-web-engine-0.2.6.0b0 geckodriver-autoinstaller-0.1.0 python-interface-1.6.1 request-1.0.117 xvfbwrapper-0.2.9
```

Repair suggestion: delete version 0.2.0b0~0.2.6.0b0 in PyPI

yllipriftI commented on Jul 7 Owner

Old releases removed from PyPi

 **ylliprifti** closed this as completed on Jul 7

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants