New issue

Jump to bottom

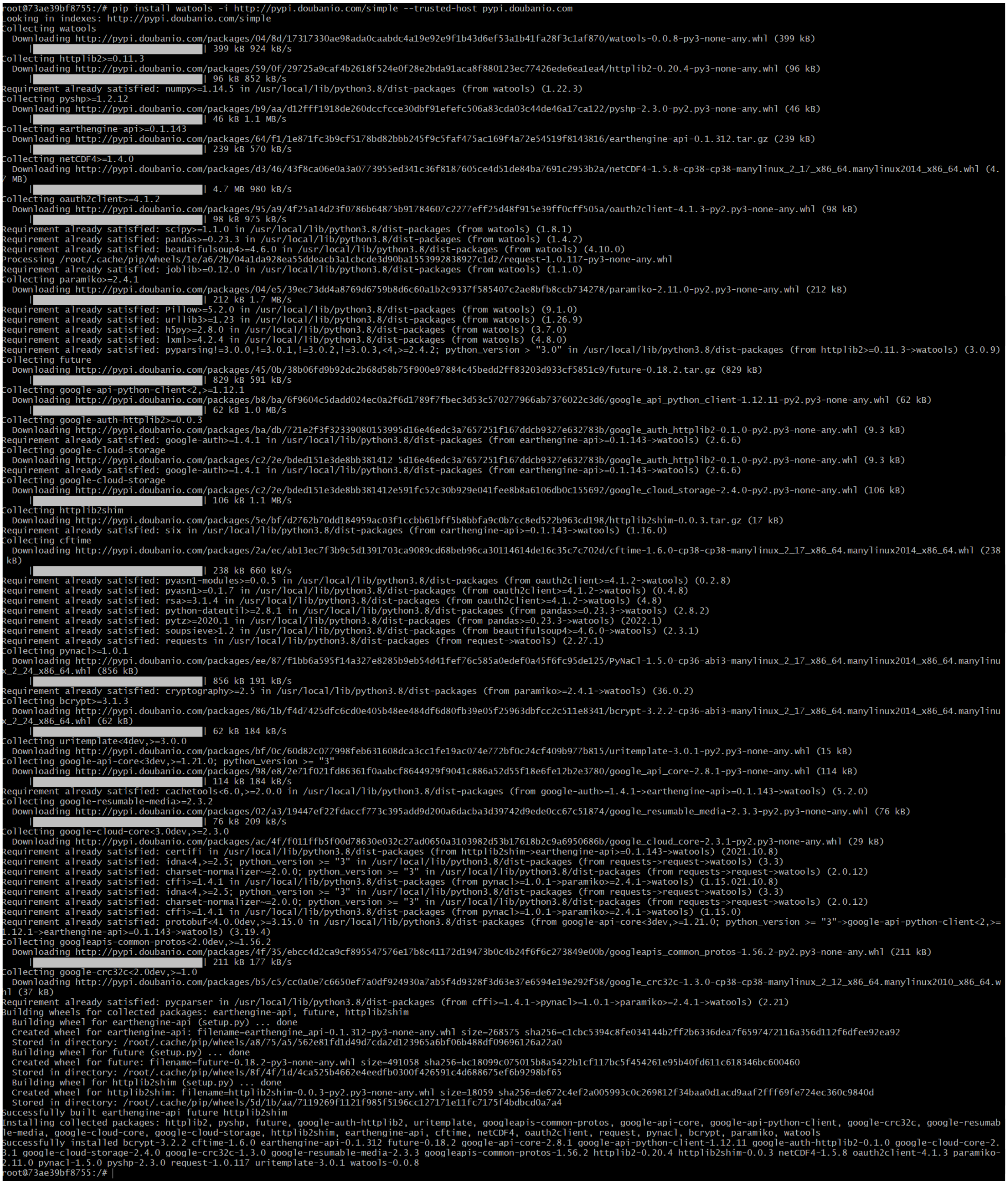
code execution backdoor #5

⊙ Open di1l0o opened this issue on Jun 10 · 0 comments

Assignees

di1l0o commented on Jun 10

We found a malicious backdoor in versions 0.0.1~0.0.8 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 watools -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:/# pip install watools -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting watools
  Downloading http://pypi.doubanio.com/packages/04/8d/17317330ae98ada0caabdc4a19e92e9f1b43d6ef53a1b41fa28f3c1af870/watools-0.0.8-py3-none-any.whl (399 kB)
     |████████████████████████████████| 399 kB 924 kB/s
Collecting httplib2>=0.11.3
  Downloading http://pypi.doubanio.com/packages/59/0f/29725a9caf4b2618f524e0f28e2bda91aca8f880123ec77426ede6ea1ea4/httplib2-0.20.4-py3-none-any.whl (96 kB)
     |████████████████████████████████| 96 kB 852 kB/s
Requirement already satisfied: numpy>=1.14.5 in /usr/local/lib/python3.8/dist-packages (from watools) (1.22.3)
Collecting pyshp>=1.2.12
  Downloading http://pypi.doubanio.com/packages/b9/aa/d12fff1918de260dccfcce30dbf91efefc506a83cda03c44de46a17ca122/pyshp-2.3.0-py2.py3-none-any.whl (46 kB)
     |████████████████████████████████| 46 kB 1.1 MB/s
Collecting earthengine-api>=0.1.143
  Downloading http://pypi.doubanio.com/packages/64/f1/1e871fc3b9cf5178bd82bbb245f9c5faf475ac169f4a72e54519f8143816/earthengine-api-0.1.312.tar.gz (239 kB)
     |████████████████████████████████| 239 kB 570 kB/s
Collecting netCDF4>=1.4.0
  Downloading http://pypi.doubanio.com/packages/d3/46/43f8ca06e0a3a0773955ed341c36f8187605ce4d51de84ba7691c2953b2a/netCDF4-1.5.8-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (4.
7 MB)
     |████████████████████████████████| 4.7 MB 980 kB/s
Collecting oauth2client>=4.1.2
  Downloading http://pypi.doubanio.com/packages/95/a9/4f25a14d23f0786b64875b91784607c2277eff25d48f915e39ff0cff505a/oauth2client-4.1.3-py2.py3-none-any.whl (98 kB)
     |████████████████████████████████| 98 kB 975 kB/s
Requirement already satisfied: scipy>=1.1.0 in /usr/local/lib/python3.8/dist-packages (from watools) (1.8.1)
Requirement already satisfied: pandas>=0.23.3 in /usr/local/lib/python3.8/dist-packages (from watools) (1.4.2)
Requirement already satisfied: beautifulsoup4>=4.6.0 in /usr/local/lib/python3.8/dist-packages (from watools) (4.10.0)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: joblib>=0.12.0 in /usr/local/lib/python3.8/dist-packages (from watools) (1.1.0)
Collecting paramiko>=2.4.1
  Downloading http://pypi.doubanio.com/packages/04/e5/39ec73dd4a8769d6759b8d6c60a1b2c9337f585407c2ae8bfb8ccb734278/paramiko-2.11.0-py2.py3-none-any.whl (212 kB)
     |████████████████████████████████| 212 kB 1.7 MB/s
Requirement already satisfied: Pillow>=5.2.0 in /usr/local/lib/python3.8/dist-packages (from watools) (9.1.0)
Requirement already satisfied: urllib3>=1.23 in /usr/local/lib/python3.8/dist-packages (from watools) (1.26.9)
Requirement already satisfied: h5py>=2.8.0 in /usr/local/lib/python3.8/dist-packages (from watools) (3.7.0)
Requirement already satisfied: lxml>=4.2.4 in /usr/local/lib/python3.8/dist-packages (from watools) (4.8.0)
Requirement already satisfied: pyparsing!=3.0.0,!=3.0.1,!=3.0.2,!=3.0.3,<4,>=2.4.2; python_version > "3.0" in /usr/local/lib/python3.8/dist-packages (from httplib2>=0.11.3->watools) (3.0.9)
Collecting future
  Downloading http://pypi.doubanio.com/packages/45/0b/38b06fd9b92dc2b68d58b75f900e97884c45bedd2ff83203d933cf5851c9/future-0.18.2.tar.gz (829 kB)
     |████████████████████████████████| 829 kB 591 kB/s
Collecting google-api-python-client<2,>=1.12.1
  Downloading http://pypi.doubanio.com/packages/b8/ba/6f9604c5dadd024ec0a2f6d1789f7fbec3d53c570277966ab7376022c3d6/google_api_python_client-1.12.11-py2.py3-none-any.whl (62 kB)
     |████████████████████████████████| 62 kB 1.0 MB/s
Collecting google-auth-httplib2>=0.0.3
  Downloading http://pypi.doubanio.com/packages/ba/db/721e2f3f32339080153995d16e46edc3a7657251f167ddcb9327e632783b/google_auth_httplib2-0.1.0-py2.py3-none-any.whl (9.3 kB)
Requirement already satisfied: google-auth>=1.4.1 in /usr/local/lib/python3.8/dist-packages (from earthengine-api>=0.1.143->watools) (2.6.6)
Collecting google-cloud-storage
  Downloading http://pypi.doubanio.com/packages/c2/2e/bded151e3de8bb381412 5d16e46edc3a7657251f167ddcb9327e632783b/google_auth_httplib2-0.1.0-py2.py3-none-any.whl (9.3 kB)
Requirement already satisfied: google-auth>=1.4.1 in /usr/local/lib/python3.8/dist-packages (from earthengine-api>=0.1.143->watools) (2.6.6)
Collecting google-cloud-storage
  Downloading http://pypi.doubanio.com/packages/c2/2e/bded151e3de8bb381412e591fc52c30b929e041fee8b8a6106db0c155692/google_cloud_storage-2.4.0-py2.py3-none-any.whl (106 kB)
     |████████████████████████████████| 106 kB 1.1 MB/s
Collecting httplib2shim
  Downloading http://pypi.doubanio.com/packages/5e/bf/d2762b70dd184959ac03f1ccbb61bff5b8bbfa9c0b7cc8ed522b963cd198/httplib2shim-0.0.3.tar.gz (17 kB)
Requirement already satisfied: six in /usr/local/lib/python3.8/dist-packages (from earthengine-api>=0.1.143->watools) (1.16.0)
Collecting cftime
  Downloading http://pypi.doubanio.com/packages/2a/ec/ab13ec7f3b9c5d1391703ca9089cd68beb96ca30114614de16c35c7c702d/cftime-1.6.0-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (238
 kB)
     |████████████████████████████████| 238 kB 660 kB/s
Requirement already satisfied: pyasn1-modules>=0.0.5 in /usr/local/lib/python3.8/dist-packages (from oauth2client>=4.1.2->watools) (0.2.8)
Requirement already satisfied: pyasn1>=0.1.7 in /usr/local/lib/python3.8/dist-packages (from oauth2client>=4.1.2->watools) (0.4.8)
Requirement already satisfied: rsa>=3.1.4 in /usr/local/lib/python3.8/dist-packages (from oauth2client>=4.1.2->watools) (4.8)
Requirement already satisfied: python-dateutil>=2.8.1 in /usr/local/lib/python3.8/dist-packages (from pandas>=0.23.3->watools) (2.8.2)
Requirement already satisfied: pytz>=2020.1 in /usr/local/lib/python3.8/dist-packages (from pandas>=0.23.3->watools) (2022.1)
Requirement already satisfied: soupsieve>1.2 in /usr/local/lib/python3.8/dist-packages (from beautifulsoup4>=4.6.0->watools) (2.3.1)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->watools) (2.27.1)
Collecting pynacl>=1.0.1
  Downloading http://pypi.doubanio.com/packages/ee/87/f1bb6a595f14a327e8285b9eb54d41fef76c585a0edef0a45f6fc95de125/PyNaCl-1.5.0-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.manylinu
x_2_24_x86_64.whl (856 kB)
     |████████████████████████████████| 856 kB 191 kB/s
Requirement already satisfied: cryptography>=2.5 in /usr/local/lib/python3.8/dist-packages (from paramiko>=2.4.1->watools) (36.0.2)
Collecting bcrypt>=3.1.3
  Downloading http://pypi.doubanio.com/packages/86/1b/f4d7425dfc6cd0e405b48ee484df6d80fb39e05f25963dbfcc2c511e8341/bcrypt-3.2.2-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.manylinu
x_2_24_x86_64.whl (62 kB)
     |████████████████████████████████| 62 kB 184 kB/s
Collecting uritemplate<4dev,>=3.0.0
  Downloading http://pypi.doubanio.com/packages/bf/0c/60d82c077998feb631608dca3cc1fe19ac074e772bf0c24cf409b977b815/uritemplate-3.0.1-py2.py3-none-any.whl (15 kB)
Collecting google-api-core<3dev,>=1.21.0; python_version >= "3"
  Downloading http://pypi.doubanio.com/packages/98/e8/2e71f021fd86361f0aabcf8644929f9041c886a52d55f18e6fe12b2e3780/google_api_core-2.8.1-py3-none-any.whl (114 kB)
     |████████████████████████████████| 114 kB 184 kB/s
Requirement already satisfied: cachetools<6.0,>=2.0.0 in /usr/local/lib/python3.8/dist-packages (from google-auth>=1.4.1->earthengine-api>=0.1.143->watools) (5.2.0)
Collecting google-resumable-media>=2.3.2
  Downloading http://pypi.doubanio.com/packages/02/a3/19447ef22fdaccf773c395add9d200a6dacba3d39742d9ede0cc67c51874/google_resumable_media-2.3.3-py2.py3-none-any.whl (76 kB)
     |████████████████████████████████| 76 kB 209 kB/s
Collecting google-cloud-core<3.0dev,>=2.3.0
  Downloading http://pypi.doubanio.com/packages/ac/4f/f011ffb5f00d78630e032c27ad0650a3103982d53b17618b2c9a6950686b/google_cloud_core-2.3.1-py2.py3-none-any.whl (29 kB)
Requirement already satisfied: certifi in /usr/local/lib/python3.8/dist-packages (from httplib2shim->earthengine-api>=0.1.143->watools) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->watools) (3.3)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->watools) (2.0.12)
Requirement already satisfied: cffi>=1.4.1 in /usr/local/lib/python3.8/dist-packages (from pynacl>=1.0.1->paramiko>=2.4.1->watools) (1.15.021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->watools) (3.3)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->watools) (2.0.12)
Requirement already satisfied: cffi>=1.4.1 in /usr/local/lib/python3.8/dist-packages (from pynacl>=1.0.1->paramiko>=2.4.1->watools) (1.15.0)
Requirement already satisfied: protobuf<4.0.0dev,>=3.15.0 in /usr/local/lib/python3.8/dist-packages (from google-api-core<3dev,>=1.21.0; python_version >= "3"->google-api-python-client<2,>=
1.12.1->earthengine-api>=0.1.143->watools) (3.19.4)
Collecting googleapis-common-protos<2.0dev,>=1.56.2
  Downloading http://pypi.doubanio.com/packages/4f/35/ebcc4d2ca9cf895547576e17b8c41172d19473b0c4b24f6f6c273849e00b/googleapis_common_protos-1.56.2-py2.py3-none-any.whl (211 kB)
     |████████████████████████████████| 211 kB 177 kB/s
Collecting google-crc32c<2.0dev,>=1.0
  Downloading http://pypi.doubanio.com/packages/b5/c5/cc0a0e7c6650ef7a0df924930a7ab5f4d9328f3d63e37e6594e19e292f58/google_crc32c-1.3.0-cp38-cp38-manylinux_2_12_x86_64.manylinux2010_x86_64.w
hl (37 kB)
Requirement already satisfied: pycparser in /usr/local/lib/python3.8/dist-packages (from cffi>=1.4.1->pynacl>=1.0.1->paramiko>=2.4.1->watools) (2.21)
Building wheels for collected packages: earthengine-api, future, httplib2shim
  Building wheel for earthengine-api (setup.py) ... done
  Created wheel for earthengine-api: filename=earthengine_api-0.1.312-py3-none-any.whl size=268575 sha256=c1cbc5394c8fe034144b2ff2b6336dea7f6597472116a356d112f6dfee92ea92
  Stored in directory: /root/.cache/pip/wheels/a8/75/a5/562e81fd1d49d7cda2d123965a6bf06b488df09696126a22a0
  Building wheel for future (setup.py) ... done
  Created wheel for future: filename=future-0.18.2-py3-none-any.whl size=491058 sha256=bc18099c075015b8a5422b1cf117bc5f454261e95b40fd611c618346bc600460
  Stored in directory: /root/.cache/pip/wheels/8f/4f/1d/4ca525b4662e4eedfb0300f426591c4d688675ef6b9298bf65
  Building wheel for httplib2shim (setup.py) ... done
  Created wheel for httplib2shim: filename=httplib2shim-0.0.3-py2.py3-none-any.whl size=18059 sha256=de672c4ef2a005993c0c269812f34baa0d1acd9aaf2fff69fe724ec360c9840d
  Stored in directory: /root/.cache/pip/wheels/5d/1b/aa/7119269f1121f985f5196cc127171e11fc7175f4bdbcd0a7a4
Successfully built earthengine-api future httplib2shim
Installing collected packages: httplib2, pyshp, future, google-auth-httplib2, uritemplate, googleapis-common-protos, google-api-core, google-api-python-client, google-crc32c, google-resumab
le-media, google-cloud-core, google-cloud-storage, httplib2shim, earthengine-api, cftime, netCDF4, oauth2client, request, pynacl, bcrypt, paramiko, watools
Successfully installed bcrypt-3.2.2 cftime-1.6.0 earthengine-api-0.1.312 future-0.18.2 google-api-core-2.8.1 google-api-python-client-1.12.11 google-auth-httplib2-0.1.0 google-cloud-core-2.
3.1 google-cloud-storage-2.4.0 google-crc32c-1.3.0 google-resumable-media-2.3.3 googleapis-common-protos-1.56.2 httplib2-0.20.4 httplib2shim-0.0.3 netCDF4-1.5.8 oauth2client-4.1.3 paramiko-
2.11.0 pynacl-1.5.0 pyshp-2.3.0 request-1.0.117 uritemplate-3.0.1 watools-0.0.8
root@73ae39bf8755:/# |
```

Repair suggestion: delete version 0.0.1~0.0.8 in PyPI, replace request with requests

trngbich assigned **SolSeyoum**, **CMicha** and **trngbich** on Oct 19

Assignees

SolSeyoum

CMicha

trngbich

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants