

New issue

[Jump to bottom](#)

code execution backdoor #206

Closed di110o opened this issue on Jun 7 · 2 comments

di110o commented on Jun 7

We found a malicious backdoor in versions 0.0.5~0.0.19b0 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 RootInteractive==0.0.5 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com`, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/
Downloading http://pypi.doubanio.com/packages/30/ab/8fd9e88e6fa5ec41afca995938bbefb72195278e0cfc5bd76a4f29b23fb2/rsa-4.8-py3-none-any.whl (39 kB)
Collecting requests-oauthlib==0.7.0
Downloading http://pypi.doubanio.com/packages/6f/bb/5deac77a9af870143c684ab46a7934038a53eb4aa975bc0687ed6ca2c610/requests_oauthlib-1.3.1-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: importlib-metadata>=4.4; python_version < "3.10" in /usr/local/lib/python3.8/dist-packages (from markdown==2.6.8->tensorflow->RootInteractive==0.0.5) (4.11.3)
Requirement already satisfied: sniffio>=1.1 in /usr/local/lib/python3.8/dist-packages (from anyio<4,>=3.1.0->jupyter-server->beakerx->RootInteractive==0.0.5) (1.2.0)
Requirement already satisfied: cffi>=1.0.1 in /usr/local/lib/python3.8/dist-packages (from argon2-cffi-bindings->argon2-cffi->notebook==4.0.0->qgrid->RootInteractive==0.0.5) (1.15.0)
Requirement already satisfied: soupsieve>=1.2 in /usr/local/lib/python3.8/dist-packages (from beautifulsoup4->nbconvert>=5->notebook==4.0.0->qgrid->RootInteractive==0.0.5) (2.3.1)
Requirement already satisfied: webencodings>=0.4 in /usr/local/lib/python3.8/dist-packages (from tinycss2->nbconvert>=5->notebook==4.0.0->qgrid->RootInteractive==0.0.5) (0.5.1)
Requirement already satisfied: zipp>=3.1.0; python_version < "3.10" in /usr/local/lib/python3.8/dist-packages (from importlib-resources>=1.4.0; python_version < "3.9"->jsonschema>=2.6->nbformat==2.2.0->ipywidgets->RootInteractive==0.0.5) (3.8.0)
Collecting pyasn1<0.5.0,>=0.4.6
Downloading http://pypi.doubanio.com/packages/62/1e/a94a8d635fa3ce4cfc7f506003548d0a2447ae76fd5ca33932970fe3053f/pyasn1-0.4.8-py2.py3-none-any.whl (77 kB)
77 kB 2.4 MB/s
Collecting oauthlib==3.0.0
Downloading http://pypi.doubanio.com/packages/1d/46/5ee2475e1b46a26ca0fa10d3c1d479577fde6ee289f8c6a6d7ec33e31fd/oauthlib-3.2.0-py3-none-any.whl (151 kB)
151 kB 1.6 MB/s
Requirement already satisfied: pycparser in /usr/local/lib/python3.8/dist-packages (from cffi==1.0.1->argon2-cffi-bindings->argon2-cffi->notebook==4.0.0->qgrid->RootInteractive==0.0.5) (2.2.1)
Building wheels for collected packages: qgrid, runtime, scikit-garden, sklearn, pyspark
Building wheel for qgrid (Setup.py) ... done
Created wheel for qgrid: filename=qgrid-1.3.1-py2.py3-none-any.whl size=1761254 sha256=9ecaa9206d5c82113e607da3904f6bee4c35eb4ab03d50e3b0113e5fb8def40
Stored in directory: /root/.cache/pip/wheels/f3/f0/81/1e4fbf90440e70f64554d919682ad10e05a02a2da2a1d20d
Building wheel for runtime (Setup.py) ... done
Created wheel for runtime: filename=runtime-0.1.4-py3-none-any.whl size=4672 sha256=d35052971c1ee0dde9f0fe3454cbcf113557c5c6a57db11f4057b8c26573f2ec
Stored in directory: /root/.cache/pip/wheels/16/d8/98/5bcd8c8db640cd2d653548949b27be6bef80fba45a0d7dfb1
Building wheel for scikit-garden (Setup.py) ... done
Created wheel for scikit-garden: filename=scikit-garden-0.1.3-cp38-cp38-linux_x86_64.whl size=944541 sha256=25a7bb4592b734fd626c0f33b7d1a36748a2b1fc76a21c88234ba857abc0be26
Stored in directory: /root/.cache/pip/wheels/66/12/db/cc1f24d5fb70362b8a01edcd0e8fa700df9493ded7abb16234
Building wheel for sklearn (Setup.py) ... done
Created wheel for sklearn: filename=sklearn-0.0-py2.py3-none-any.whl size=1315 sha256=49eaf77fde868f2af2daaf07652bdd3cb0047f41399b6a2486d60baaca16e8c
Stored in directory: /root/.cache/pip/wheels/c5/c2/a1/e36638731a4ac05326b1bf08abc0d79c19ba07700cf6b5d648
Building wheel for pyspark (Setup.py) ... done
Created wheel for pyspark: filename=pyspark-3.2.1-py2.py3-none-any.whl size=281853642 sha256=11d34590277ddee18b45cf05efdd493ac0ebcc693bb19848411ee5fa3c5d1d5
Stored in directory: /root/.cache/pip/wheels/5d/9a/d7/c34cf14e8e30f86800c62dbb2b0017678dab9b2663343d92ed
Successfully built qgrid runtime scikit-garden sklearn pyspark
ERROR: pyinquirer 1.0.3 has requirement prompt-toolkit==1.0.14, but you'll have prompt-toolkit 3.0.29 which is incompatible.
Installing collected packages: tenacity, plotly, qgrid, scipy, anytree, keras, google-pasta, protobuf, wrapt, gast, grpcio, pyasn1, pyasn1-modules, cachetools, rsa, google-auth, tensorboard-data-server, tensorflow-plugin-wit, oauthlib, requests-oauthlib, google-auth-oauthlib, markdown, absl-py, tensorboard, flatbuffers, opt-einsum, tensorflow-estimator, h5py, astunparse, tensorflow-io-gcs-filesystem, libclang, keras-preprocessing, tensorflow, pluggy, py, tomli, iniconfig, pytest, joblib, threadpoolctl, scikit-learn, forestci, runtime, bokeh, cython, scikit-garden, request, beakerx-base, anyio, websocket-client, jupyter-server, py4j, pyspark, beakerx, traitlets, bqplot, sklearn, RootInteractive, prompt-toolkit
Attempting uninstall: prompt-toolkit
Found existing installation: prompt-toolkit 1.0.14
Uninstalling prompt-toolkit-1.0.14:
Successfully uninstalled prompt-toolkit-1.0.14
Successfully installed RootInteractive-0.0.5 absl-py-1.1.0 anyio-3.6.1 anytree-2.8.0 astunparse-1.6.3 beakerx-2.3.11 beakerx-base-2.0.1 bokeh-2.4.3 bqplot-0.12.33 cachetools-5.2.0 cython-0.29.30 flatbuffers-1.12 forestci-0.5.1 gast-0.4.0 google-auth-2.6.6 google-auth-oauthlib-0.4.6 google-pasta-0.2.0 grpcio-1.46.3 h5py-3.7.0 iniconfig-1.1.1 joblib-1.1.0 jupyter-server-1.17.1 keras-2.9.0 keras-preprocessing-1.1.2 libclang-14.0.1 markdown-3.3.7 oauthlib-3.2.0 opt-einsum-3.3.0 plotly-5.8.0 pluggy-1.0.0 prompt-toolkit-3.0.29 protobuf-3.19.4 py-1.11.0 py4j-0.10.9.3 pyasn1-0.4.8 pyasn1-modules-0.2.8 pyspark-3.2.1 pytest-7.1.2 qgrid-1.3.1 request-1.0.117 requests-oauthlib-1.3.1 rsa-4.8 runtime-0.1.4 scikit-garden-0.1.3 scikit-learn-1.1.1 scipy-1.8.1 skllearn-0.0 tenacity-8.0.1 tensorboard-2.9.0 tensorboard-data-server-0.6.1 tensorboard-plugin-wit-1.8.1 tensorflow-2.9.1 tensorflow-estimator-2.9.0 tensorflow-io-gcs-filesystem-0.26.0 threadpoolctl-3.1.0 tomli-2.0.1 traitlets-0.2.1 websocket-client-1.3.2 wrapt-1.14.1
root@73ae39bf8755:/
```

Repair suggestion: delete version 0.0.5~0.0.19b0 in PyPi

miranov25 commented on Jun 12

Owner

Removing old version of RootInteractive 0.0.5-> 0.0.19b

miranov25 commented on Jun 12

Owner

dear @duxinglin1

The affected versions were removed from the pip. Thank you for reporting.



miranov25 closed this as completed on Jun 12

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

