democritus-project / d8s-dates Public

<> Code   ⊙ Issues 8   Pull requests   ▷ Actions   Projects   Security   ···

New issue

Jump to bottom

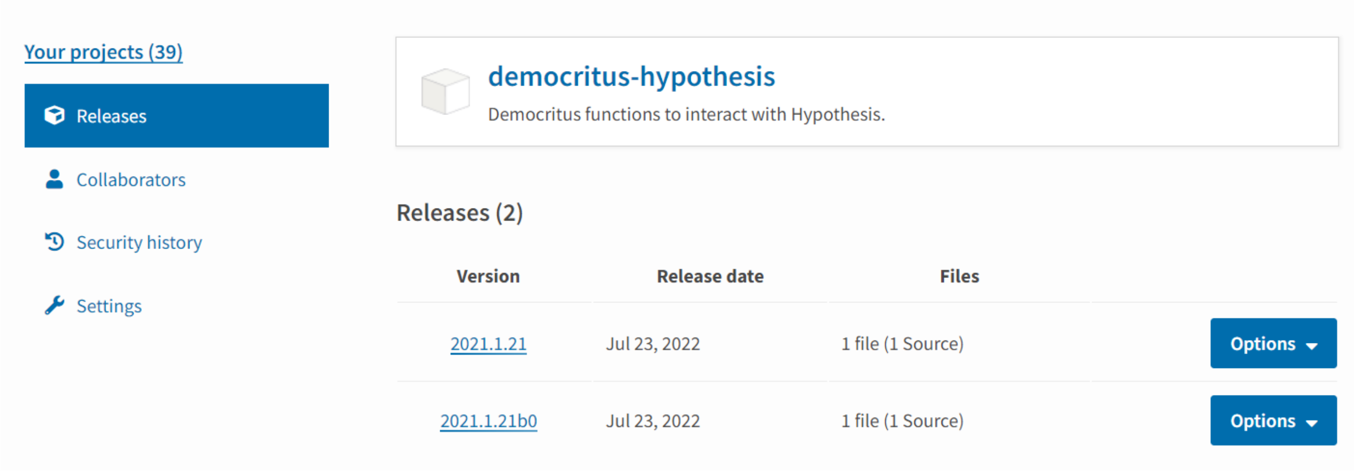
code execution backdoor #26

⊙ Open   di1l0o opened this issue on Sep 13 · 0 comments

Labels	bug
Projects	Backlog

di1l0o commented on Sep 13

We discovered a potential code execution backdoor in version 0.1.0 of the project, the backdoor is the democritus-hypothesis package. Attackers can upload democritus-hypothesis packages containing arbitrary malicious code. For the safety of this project, the democritus-hypothesis package has been uploaded by us.



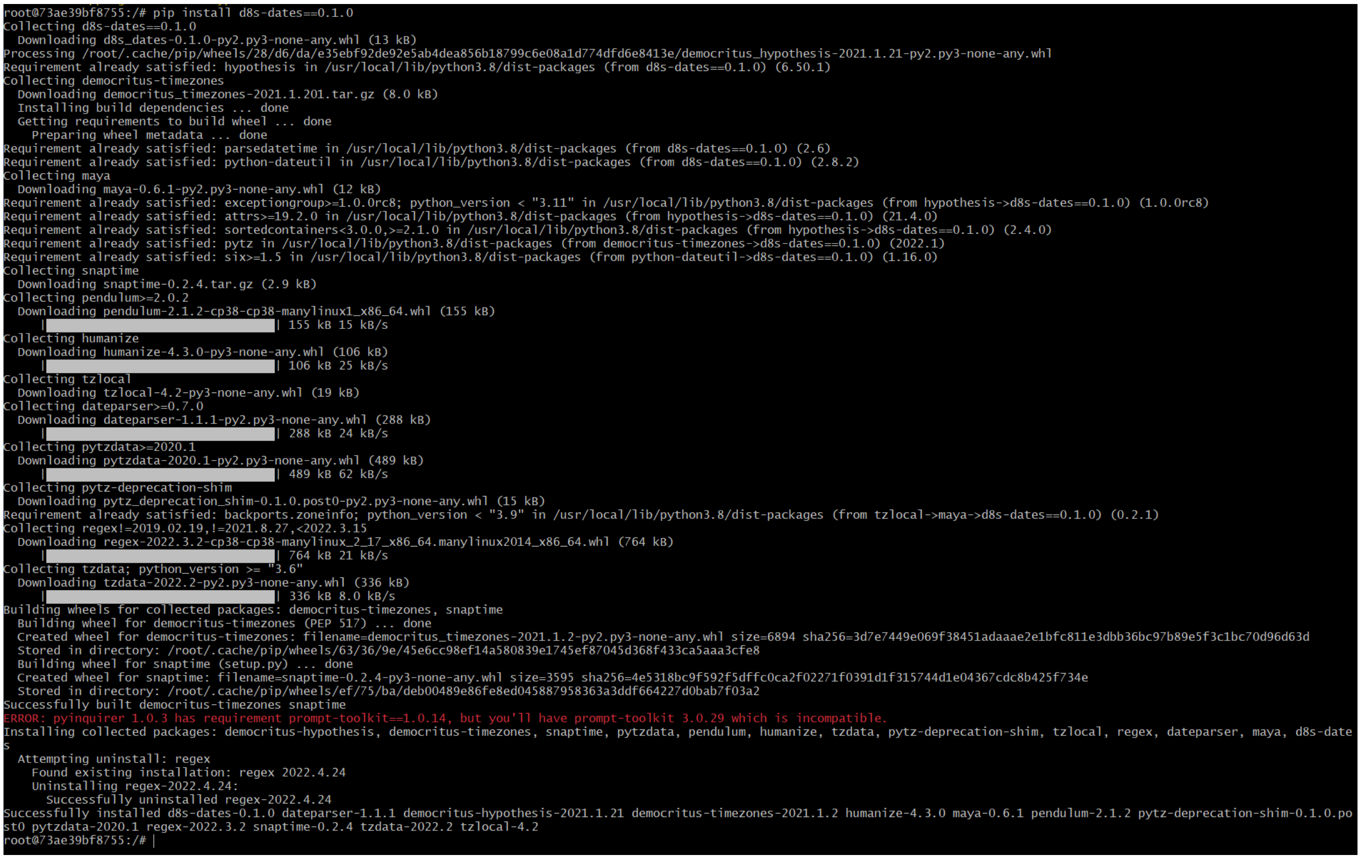
democritus-hypothesis

Democritus functions to interact with Hypothesis.

Releases (2)

Version	Release date	Files	
2021.1.21	Jul 23, 2022	1 file (1 Source)	Options ▾
2021.1.21b0	Jul 23, 2022	1 file (1 Source)	Options ▾

The democritus-hypothesis package can be successfully installed using `pip install d8s-dates==0.1.0`



```
root@73ae39bf8755:/# pip install d8s-dates==0.1.0
Collecting d8s-dates==0.1.0
  Downloading d8s_dates-0.1.0-py2.py3-none-any.whl (13 kB)
Processing /root/.cache/pip/wheels/28/d6/da/e35ebf92de92e5ab4dea856b18799c6e08a1d774dfd6e8413e/democritus_hypothesis-2021.1.21-py2.py3-none-any.whl
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-dates==0.1.0) (6.50.1)
Collecting democritus-timezones
  Downloading democritus_timezones-2021.1.201.tar.gz (8.0 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Requirement already satisfied: parsedatetime in /usr/local/lib/python3.8/dist-packages (from d8s-dates==0.1.0) (2.6)
Requirement already satisfied: python-dateutil in /usr/local/lib/python3.8/dist-packages (from d8s-dates==0.1.0) (2.8.2)
Collecting maya
  Downloading maya-0.6.1-py2.py3-none-any.whl (12 kB)
Requirement already satisfied: exceptiongroup>=1.0.0rc8; python_version < "3.11" in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-dates==0.1.0) (1.0.0rc8)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-dates==0.1.0) (21.4.0)
Requirement already satisfied: sortedcontainers<3.0.0,>=2.1.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-dates==0.1.0) (2.4.0)
Requirement already satisfied: pytz in /usr/local/lib/python3.8/dist-packages (from democritus-timezones->d8s-dates==0.1.0) (2022.1)
Requirement already satisfied: six>=1.5 in /usr/local/lib/python3.8/dist-packages (from python-dateutil->d8s-dates==0.1.0) (1.16.0)
Collecting snaptime
  Downloading snaptime-0.2.4.tar.gz (2.9 kB)
Collecting pendulum>=2.0.2
  Downloading pendulum-2.1.2-cp38-cp38-manylinux1_x86_64.whl (155 kB)
     |████████████████████████████████| 155 kB 15 kB/s
Collecting humanize
  Downloading humanize-4.3.0-py3-none-any.whl (106 kB)
     |████████████████████████████████| 106 kB 25 kB/s
Collecting tzlocal
  Downloading tzlocal-4.2-py3-none-any.whl (19 kB)
Collecting dateparser>=0.7.0
  Downloading dateparser-1.1.1-py2.py3-none-any.whl (288 kB)
     |████████████████████████████████| 288 kB 24 kB/s
Collecting pytzdata>=2020.1
  Downloading pytzdata-2020.1-py2.py3-none-any.whl (489 kB)
     |████████████████████████████████| 489 kB 62 kB/s
Collecting pytz-deprecation-shim
  Downloading pytz_deprecation_shim-0.1.0.post0-py2.py3-none-any.whl (15 kB)
Requirement already satisfied: backports.zoneinfo; python_version < "3.9" in /usr/local/lib/python3.8/dist-packages (from tzlocal->maya->d8s-dates==0.1.0) (0.2.1)
Collecting regex!=2019.02.19,!=2021.8.27,<2022.3.15
  Downloading regex-2022.3.2-cp38-cp38-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (764 kB)
     |████████████████████████████████| 764 kB 21 kB/s
Collecting tzdata; python_version >= "3.6"
  Downloading tzdata-2022.2-py2.py3-none-any.whl (336 kB)
     |████████████████████████████████| 336 kB 8.0 kB/s
Building wheels for collected packages: democritus-timezones, snaptime
  Building wheel for democritus-timezones (PEP 517) ... done
  Created wheel for democritus-timezones: filename=democritus_timezones-2021.1.2-py2.py3-none-any.whl size=6894 sha256=3d7e7449e069f38451adaaae2e1bfc811e3dbb36bc97b89e5f3c1bc70d96d63d
  Stored in directory: /root/.cache/pip/wheels/63/36/9e/45e6cc98ef14a580839e1745ef87045d368f433ca5aaa3cfe8
  Building wheel for snaptime (setup.py) ... done
  Created wheel for snaptime: filename=snaptime-0.2.4-py3-none-any.whl size=3595 sha256=4e5318bc9f592f5dffc0ca2f02271f0391d1f315744d1e04367cdc8b425f734e
  Stored in directory: /root/.cache/pip/wheels/ef/75/ba/deb00489e86fe8ed045887958363a3ddf664227d0bab7f03a2
Successfully built democritus-timezones snaptime
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: democritus-hypothesis, democritus-timezones, snaptime, pytzdata, pendulum, humanize, tzdata, pytz-deprecation-shim, tzlocal, regex, dateparser, maya, d8s-date
s
  Attempting uninstall: regex
    Found existing installation: regex 2022.4.24
    Uninstalling regex-2022.4.24:
      Successfully uninstalled regex-2022.4.24
Successfully installed d8s-dates-0.1.0 dateparser-1.1.1 democritus-hypothesis-2021.1.21 democritus-timezones-2021.1.2 humanize-4.3.0 maya-0.6.1 pendulum-2.1.2 pytz-deprecation-shim-0.1.0.po
st0 pytzdata-2020.1 regex-2022.3.2 snaptime-0.2.4 tzdata-2022.2 tzlocal-4.2
root@73ae39bf8755:/# |
```

Suggestion: remove version 0.1.0 of this project in PyPI

👀 1

di1l0o added the bug label on Sep 13

fhightower added this to **To do** in **Backlog** on Sep 13

Assignees

No one assigned

Labels

bug

Projects

Backlog
To do

Milestone

No milestone

Development

No branches or pull requests

1 participant