democritus-project / d8s-uuids Public

<> Code ⊙ Issues 1 Pull requests ▷ Actions Projects Security ···

New issue

Jump to bottom

code execution backdoor #5

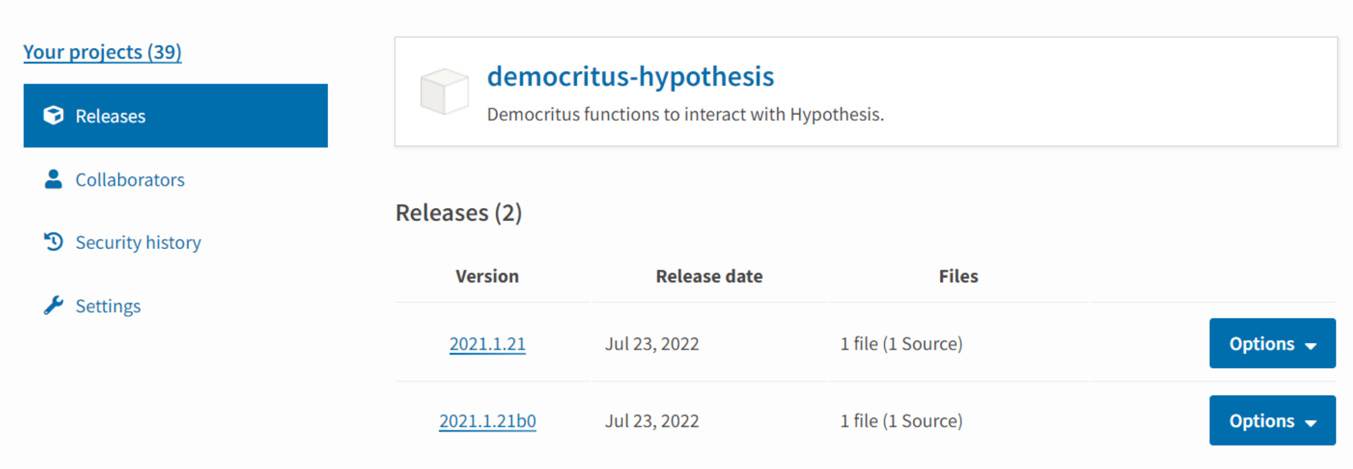
⊙ Open di1l0o opened this issue on Sep 13 · 0 comments

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.



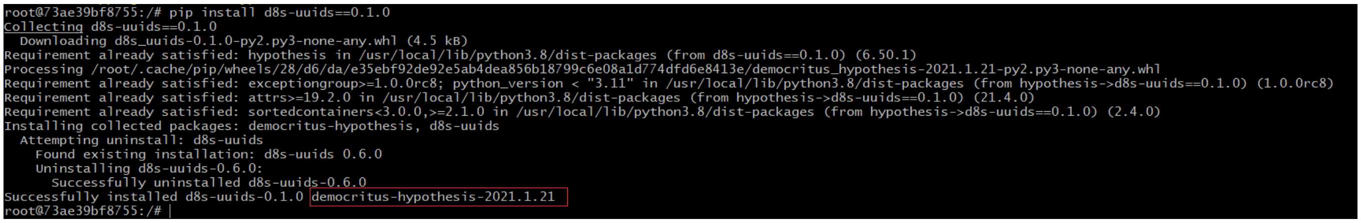
democritus-hypothesis

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-uuids==0.1.0`



```
root@73ae39bf8755:/# pip install d8s-uuids==0.1.0
Collecting d8s-uuids==0.1.0
  Downloading d8s_uuids-0.1.0-py2.py3-none-any.whl (4.5 kB)
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-uuids==0.1.0) (6.50.1)
Processing /root/.cache/pip/wheels/28/d6/da/e35ebf92de92e5ab4dea856b18799c6e08a1d774dfd6e8413e/democritus_hypothesis-2021.1.21-py2.py3-none-any.whl
Requirement already satisfied: exceptiongroup>=1.0.0rc8; python_version < "3.11" in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-uuids==0.1.0) (1.0.0rc8)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-uuids==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-uuids==0.1.0) (2.4.0)
Installing collected packages: democritus-hypothesis, d8s-uuids
  Attempting uninstall: d8s-uuids
    Found existing installation: d8s-uuids 0.6.0
    Uninstalling d8s-uuids-0.6.0:
      Successfully uninstalled d8s-uuids-0.6.0
Successfully installed d8s-uuids-0.1.0 democritus-hypothesis-2021.1.21
root@73ae39bf8755:/# |
```

Suggestion: remove version 0.1.0 of this project in PyPI

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