<> Code   ⊙ **Issues** 10   ⫙ Pull requests   ▷ Actions   ▦ Projects   ⦸ Security   •••

New issue   Jump to bottom

code execution backdoor #21

⊘ **Closed**   **di1l0o** opened this issue on Sep 11 · 0 comments

Labels	bug
Projects	⊞ Backlog

di1l0o commented on Sep 11

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.

Your projects (39)

📦 Releases
👤 Collaborators
🕘 Security history
🔧 Settings

📦 **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-strings==0.1.0`

```
root@73ae39bf8755:/# pip install d8s-strings==0.1.0
Collecting d8s-strings==0.1.0
  Downloading d8s_strings-0.1.0-py2.py3-none-any.whl (21 kB)
Collecting democritus-hypothesis
  Downloading democritus_hypothesis-2021.1.2101.tar.gz (6.1 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Requirement already satisfied: inflect in /usr/local/lib/python3.8/dist-packages (from d8s-strings==0.1.0) (5.6.1)
Requirement already satisfied: more-itertools in /usr/local/lib/python3.8/dist-packages (from d8s-strings==0.1.0) (8.13.0)
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-strings==0.1.0) (6.50.1)
Requirement already satisfied: democritus-uuids in /usr/local/lib/python3.8/dist-packages (from d8s-strings==0.1.0) (2021.1.21)
Requirement already satisfied: exceptiongroup>=1.0.0rc8; python_version < "3.11" in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-strings==0.1.0) (1.0.0rc8)
Requirement already satisfied: sortedcontainers<3.0.0,>=2.1.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-strings==0.1.0) (2.4.0)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-strings==0.1.0) (21.4.0)
Building wheels for collected packages: democritus-hypothesis
  Building wheel for democritus-hypothesis (PEP 517) ... done
  Created wheel for democritus-hypothesis: filename=democritus_hypothesis-2021.1.21-py2.py3-none-any.whl size=4755 sha256=65a993e7f1becaea92b8b44ab470b99a6ce800a419830679f8b07afdbd3e1121
  Stored in directory: /root/.cache/pip/wheels/28/d6/da/e35ebf92de92e5ab4dea856b18799c6e08a1d774dfd6e8413e
Successfully built democritus-hypothesis
ERROR: democritus-urls 2021.1.25 requires democritus-networking, which is not installed.
ERROR: democritus-html 2021.1.25 requires democritus-networking, which is not installed.
ERROR: democritus-domains 2021.1.21 requires democritus-networking, which is not installed.
ERROR: d8s-utility 0.1.0 requires democritus-networking, which is not installed.
ERROR: d8s-pdfs 0.1.0 requires democritus-networking, which is not installed.
ERROR: d8s-ip-addresses 0.1.0 requires democritus-networking, which is not installed.
ERROR: d8s-html 0.1.0 requires democritus-networking, which is not installed.
ERROR: d8s-domains 0.1.0 requires democritus-networking, which is not installed.
ERROR: d8s-asns 0.1.0 requires democritus-networking, which is not installed.
ERROR: ioc-finder 7.2.2 has requirement d8s-strings<1.0,>=0.5.0, but you'll have d8s-strings 0.1.0 which is incompatible.
Installing collected packages: democritus-hypothesis, d8s-strings
  Attempting uninstall: d8s-strings
    Found existing installation: d8s-strings 0.5.0
    Uninstalling d8s-strings-0.5.0:
      Successfully uninstalled d8s-strings-0.5.0
Successfully installed d8s-strings-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 11

🗂️ 🐱 **fhightower** added this to **To do** in **Backlog** on Sep 11

🐱 **fhightower** closed this as completed on Oct 13

Assignees

No one assigned

Labels

`bug`

Projects

🗂️ **Backlog**
To do

Milestone

No milestone

Development

No branches or pull requests

---

2 participants