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

New issue   **Jump to bottom**

code execution backdoor #10

⊘ **Closed**   **di1l0o** opened this issue on Sep 12 · 0 comments

Labels   bug

Projects   ⊞ Backlog

---

di1l0o commented on Sep 12

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)

| | democritus-hypothesis |
| | Democritus functions to interact with Hypothesis. |

Releases
Collaborators
Security history
Settings

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-urls==0.1.0`

```
root@73ae39bf8755:/# pip install d8s-urls==0.1.0
Collecting d8s-urls==0.1.0
  Using cached d8s_urls-0.1.0-py2.py3-none-any.whl (9.0 kB)
Processing /root/.cache/pip/wheels/28/d6/da/e35ebf92de92e5ab4dea856b18799c6e08a1d774dfd6e8413e/democritus_hypothesis-2021.1.21-py2.py3-none-any.whl
Requirement already satisfied: democritus-domains in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-csv in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-strings in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.28)
Requirement already satisfied: democritus-file-system in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.27)
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (6.50.1)
Requirement already satisfied: ioc-finder in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (7.2.2)
Processing /root/.cache/pip/wheels/ab/55/19/c3bed03ed46cf6d376a7e62e51f2221c3581f5492e926fddbe/democritus_networking-2021.1.21-py2.py3-none-any.whl
Requirement already satisfied: werkzeug in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2.1.2)
Requirement already satisfied: tldextract in /usr/local/lib/python3.8/dist-packages (from democritus-domains->d8s-urls==0.1.0) (3.3.1)
Requirement already satisfied: democritus-urls in /usr/local/lib/python3.8/dist-packages (from democritus-domains->d8s-urls==0.1.0) (2021.1.25)
Requirement already satisfied: whois in /usr/local/lib/python3.8/dist-packages (from democritus-domains->d8s-urls==0.1.0) (0.9.16)
Requirement already satisfied: inflect in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-urls==0.1.0) (5.6.1)
Requirement already satisfied: more-itertools in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-urls==0.1.0) (8.13.0)
Requirement already satisfied: democritus-uuids in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-hashes in /usr/local/lib/python3.8/dist-packages (from democritus-file-system->d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: atomicwrites in /usr/local/lib/python3.8/dist-packages (from democritus-file-system->d8s-urls==0.1.0) (1.4.1)
Requirement already satisfied: exceptiongroup>=1.0.0rc8; python_version < "3.11" in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-urls==0.1.0) (1.0.0rc8)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->d8s-urls==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-urls==0.1.0) (2.4.0)
Requirement already satisfied: ioc-fanger<4.0,>=3.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->d8s-urls==0.1.0) (3.4.1)
Requirement already satisfied: click<9.0,>=7.1.2 in /usr/l/lib/python3.8/dist-packages (from hypothesis->d8s-urls==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-urls==0.1.0) (2.4.0)
Requirement already satisfied: ioc-fanger<4.0,>=3.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->d8s-urls==0.1.0) (3.4.1)
Requirement already satisfied: click<9.0,>=7.1.2 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->d8s-urls==0.1.0) (8.0.4)
Requirement already satisfied: pyparsing<=3.0.9,>=3.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->d8s-urls==0.1.0) (3.0.9)
Collecting d8s-strings<1.0,>=0.5.0
  Downloading d8s_strings-0.5.0-py2.py3-none-any.whl (37 kB)
Requirement already satisfied: democritus-json in /usr/local/lib/python3.8/dist-packages (from democritus-networking->d8s-urls==0.1.0) (2021.1.25)
Requirement already satisfied: democritus-user-agents in /usr/local/lib/python3.8/dist-packages (from democritus-networking->d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from democritus-networking->d8s-urls==0.1.0) (2.27.1)
Requirement already satisfied: requests-file>=1.4 in /usr/local/lib/python3.8/dist-packages (from tldextract->democritus-domains->d8s-urls==0.1.0) (1.5.1)
Requirement already satisfied: filelock>=3.0.8 in /usr/local/lib/python3.8/dist-packages (from tldextract->democritus-domains->d8s-urls==0.1.0) (3.7.1)
Requirement already satisfied: idna in /usr/local/lib/python3.8/dist-packages (from tldextract->democritus-domains->d8s-urls==0.1.0) (2.10)
Requirement already satisfied: ppdeep in /usr/local/lib/python3.8/dist-packages (from democritus-hashes->democritus-file-system->d8s-urls==0.1.0) (20200505)
Requirement already satisfied: d8s-dicts==0.6.0 in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5. omains->d8s-urls==0.1.0) (3.7.1)
Requirement already satisfied: idna in /usr/local/lib/python3.8/dist-packages (from tldextract->democritus-domains->d8s-urls==0.1.0) (2.10)
Requirement already satisfied: ppdeep in /usr/local/lib/python3.8/dist-packages (from democritus-hashes->democritus-file-system->d8s-urls==0.1.0) (20200505)
Requirement already satisfied: d8s-dicts==0.6.0 in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.6.0)
Requirement already satisfied: d8s-lists==0.8.0 in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.8.0)
Requirement already satisfied: d8s-hypothesis==0.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.6.0)
Requirement already satisfied: d8s-uuids==0.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.6.0)
Requirement already satisfied: d8s-math==0.7.0 in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.7.0)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->d8s-urls==0.1.0) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->d8s-urls==0.1.0) (2021.10.8)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->d8s-urls==0.1.0) (1.25.11)
Requirement already satisfied: six in /usr/local/lib/python3.8/dist-packages (from requests-file>=1.4->tldextract->democritus-domains->d8s-urls==0.1.0) (1.16.0)
Requirement already satisfied: dictdiffer in /usr/local/lib/python3.8/dist-packages (from d8s-dicts==0.6.0->d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.9.0)
Requirement already satisfied: number-tools in /usr/local/lib/python3.8/dist-packages (from d8s-math==0.7.0->d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.1.0)
Requirement already satisfied: sympy in /usr/local/lib/python3.8/dist-packages (from d8s-math==0.7.0->d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (1.10.1)
Requirement already satisfied: mpmath>=0.19 in /usr/local/lib/python3.8/dist-packages (from sympy->d8s-math==0.7.0->d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (1.2.1)
Installing collected packages: democritus-hypothesis, democritus-networking, d8s-urls, d8s-strings
  Attempting uninstall: d8s-strings
    Found existing installation: d8s-strings 0.1.0
    Uninstalling d8s-strings-0.1.0:
      Successfully uninstalled d8s-strings-0.1.0
Successfully installed d8s-strings-0.5.0 d8s-urls-0.1.0 democritus-hypothesis-2021.1.21 democritus-networking-2021.1.21
root@73ae39bf8755:/#
```

Suggestion: remove version 0.1.0 of this project in PyPI

🏷️ **di1l0o** added the `bug` label on Sep 12

🗔 **fhightower** added this to **To do** in **Backlog** on Sep 12

fhightower closed this as completed on Sep 24

Assignees

No one assigned

Labels

bug

Projects

🗔 **Backlog**
   To do

Milestone

No milestone

Development

No branches or pull requests

---

2 participants