

New issue

[Jump to bottom](#)

code execution backdoor #12

✓ Closed di1l0o opened this issue on Sep 23 · 0 comments

Labels bug

Projects Backlog

di1l0o commented on Sep 23

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

[Your projects \(39\)](#)

Releases

Collaborators

Security history

Settings



democritus-csv

Democritus functions for working with CSV.

Releases (1)


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

The democritus-csv package can be successfully installed using `pip install d8s-urls==0.1.0`

```
root@73ae39bf8755:/# pip install d8s-urls==0.1.0
Requirement already satisfied: d8s-urls==0.1.0 in /usr/local/lib/python3.8/dist-packages (0.1.0)
Requirement already satisfied: ioc-finder in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (7.2.2)
Requirement already satisfied: democritus-hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.21)
Requirement already satisfied: werkzeug in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2.1.2)
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (6.50.1)
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-networking in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.21)
Collecting democritus-csv
  Downloading democritus_csv-2021.1.2101.tar.gz (6.0 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing wheel metadata ... done
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-file-system in /usr/local/lib/python3.8/dist-packages (from d8s-urls==0.1.0) (2021.1.27)
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)
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: d8s-strings<1.0,>=0.5.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->d8s-urls==0.1.0) (0.5.0)
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: 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: 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-networking->d8s-urls==0.1.0) (2021.1.21)
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: democritus-json in /usr/local/lib/python3.8/dist-packages (from democritus-networking->d8s-urls==0.1.0) (2021.1.25)
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: whois in /usr/local/lib/python3.8/dist-packages (from democritus-domains->d8s-urls==0.1.0) (0.9.16)
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: tldextract in /usr/local/lib/python3.8/dist-packages (from democritus-domains->d8s-urls==0.1.0) (3.3.1)
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: 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: d8s-uuids==0.7.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->d8s-urls==0.1.0) (0.1.0)
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-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: ppdeep in /usr/local/lib/python3.8/dist-packages (from democritus-hashes->democritus-networking->d8s-urls==0.1.0) (20200505)
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: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->d8s-urls==0.1.0) (2.10)
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: 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: 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: 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: 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: 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: 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: 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)
Building wheels for collected packages: democritus-csv
  Building wheel for democritus-csv (PEP 517) ... done
  Created wheel for democritus-csv: filename=democritus_csv-2021.1.21-py2.py3-none-any.whl size=4689 sha256=e2bd37599d085c46389bb5e123717572c232a9ab4f21c2dc0cf568e949df896d
  Stored in directory: /root/.cache/pip/wheels/c5/99/25/586593788d1a815789ade32e51a425063f143cf2d6bf907d4a
Successfully built democritus-csv
Installing collected packages: democritus-csv
Successfully installed democritus-csv-2021.1.21
root@73ae39bf8755:/#
```

Suggestion: remove version 0.1.0 of this project in PyPI

  di110o added the **bug** label on Sep 23

  fhightower added this to **To do in Backlog** on Sep 23

 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

