<> Code   ⊙ Issues 2   ⫦ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   ···

New issue   Jump to bottom

code execution backdoor #10

⊘ Closed   **di1l0o** opened this issue on Aug 26 · 1 comment

Labels   bug

Projects   ⊞ Backlog

---

di1l0o commented on Aug 26

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

democritus-strings

Democritus functions for working with Python strings.

Releases (1)

Version	Release date	Files	
2021.1.28	Jul 23, 2022	1 file (1 Source)	**Options** ▾

The democritus-strings package can be successfully installed using `pip install d8s-xml==0.1.0`

```
root@73ae39bf8755:/# pip install d8s-xml==0.1.0
Collecting d8s-xml==0.1.0
  Downloading d8s_xml-0.1.0-py2.py3-none-any.whl (5.5 kB)
  Processing /root/.cache/pip/wheels/90/c5/06/11a9574033331d0ccb72559d9afc25564336f0024d8a19c40f/democritus_strings-2021.1.28-py2.py3-none-any.whl
Collecting democritus-html
  Downloading democritus_html-2021.1.2501.tar.gz (9.4 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Collecting democritus-utility
  Downloading democritus_utility-2021.1.3001.tar.gz (10 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Requirement already satisfied: hypothesis in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (6.50.1)
Requirement already satisfied: more-itertools in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (8.13.0)
Requirement already satisfied: inflect in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (5.6.1)
Requirement already satisfied: democritus-uuids in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-hypothesis in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-urls in /usrib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (5.6.1)
Requirement already satisfied: democritus-uuids in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-hypothesis in /usr/local/lib/python3.8/dist-packages (from democritus-strings->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-urls in /usr/local/lib/python3.8/dist-packages (from democritus-html->d8s-xml==0.1.0) (2021.1.25)
Collecting html2text
  Downloading html2text-2020.1.16-py3-none-any.whl (32 kB)
Collecting html-to-json
  Downloading html_to_json-2.0.0-py2.py3-none-any.whl (6.4 kB)
Requirement already satisfied: beautifulsoup4 in /usr/local/lib/python3.8/dist-packages (from democritus-html->d8s-xml==0.1.0) (4.10.0)
Requirement already satisfied: democritus-networking in /usr/local/lib/python3.8/dist-packages (from democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-file-system in /usr/local/lib/python3.8/dist-packages (from democritus-utility->d8s-xml==0.1.0) (2021.1.27)
Collecting democritus-lists
  Downloading democritus_lists-2021.1.2101.tar.gz (10 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Requirement already satisfied: sortedcontainers<3.0.0,>=2.1.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->democritus-strings->d8s-xml==0.1.0) (2.4.0)
Requirement already satisfied: exceptiongroup>=1.0.0rc8; python_version < "3.11" in /usr/local/lib/python3.8/dist-packages (from hypothesis->democritus-strings->d8s-xml==0.1.0) (1.0.0rc8)
Requirement already satisfied: attrs>=19.2.0 in /usr/local/lib/python3.8/dist-packages (from hypothesis->democritus-strings->d8s-xml==0.1.0) (21.4.0)
Requirement already satisfied: democritus-domains in /usr/local/lib/python3.8/dist-packages (from democritus-urls->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: ioc-finder in /usr/local/lib/python3.8/dist-packages (from democritus-urls->democritus-html->d8s-xml==0.1.0) (7.2.2)
Requirement already satisfied: democritus-csv in /usr/local/lib/python3.8/dist-packages (from democritus-urls->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: werkzeug in /usr/local/lib/python3.8/dist-packages (from democritus-urls->democritus-html->d8s-xml==0.1.0) (2.1.2)
Requirement already satisfied: bs4 in /usr/local/lib/python3.8/dist-packages (from html-to-json->democritus-html->d8s-xml==0.1.0) (0.0.1)
Requirement already satisfied: soupsieve>1.2 in /usr/local/lib/python3.8/dist-packages (from beautifulsoup4->democritus-html->d8s-xml==0.1.0) (2.3.1)
Requirement already satisfied: democritus-hashes in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-json in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.25)
Requirement already satisfied: democritus-user-agents in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: democritus-json in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.25)
Requirement already satisfied: democritus-user-agents in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2021.1.21)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from democritus-networking->democritus-html->d8s-xml==0.1.0) (2.27.1)
Requirement already satisfied: atomicwrites in /usr/local/lib/python3.8/dist-packages (from democritus-file-system->democritus-utility->d8s-xml==0.1.0) (1.4.1)
Collecting democritus-dicts
  Downloading democritus_dicts-2021.1.2101.tar.gz (10 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
    Preparing wheel metadata ... done
Requirement already satisfied: tldextract in /usr/local/lib/python3.8/dist-packages (from democritus-domains->democritus-urls->democritus-html->d8s-xml==0.1.0) (3.3.1)
Requirement already satisfied: whois in /usr/local/lib/python3.8/dist-packages (from democritus-domains->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.9.16)
Requirement already satisfied: pyparsing<=3.0.9,>=3.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->democritus-urls->democritus-html->d8s-xml==0.1.0) (3.0.9)
Requirement already satisfied: ioc-fanger<4.0,>=3.0 in /usr/local/lib/python3.8/dist-packages (from ioc-finder->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.5.0)
Requirement already satisfied: ppdeep in /usr/local/lib/python3.8/dist-packages (from democritus-hashes->democritus-networking->democritus-html->d8s-xml==0.1.0) (20200505)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->democritus-html->d8s-xml==0.1.0) (1.25.11)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->democritus-networking->democritus-html->d8s-xml==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->democritus-html->d8s-xml==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->democritus-html->d8s-xml==0.1.0) (2.10)
Requirement already satisfied: dictdiffer in /usr/local/lib/python3.8/dist-packages (from democritus-dicts->democritus-lists->democritus-utility->d8s-xml==0.1.0) (0.9.0)
Requirement already satisfied: requests-file>=1.4 in /usr/local/lib/python3.8/dist-packages (from tldextract->democritus-domains->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==0.1.0) (3.7.1)
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->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.8.0)
Requirement already satisfied: d8s-uuids==0.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.6.0)
Requirement already satisfied: d8s-hypothesis==0.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.6.0)
Requirement already satisfied: d8s-dicts==0.6.0 in /usr/local/lib/python3.8/dist-packages (from d8s-rings<1.0,>=0.5.0->ioc-finder->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.6.0)
Requirement already satisfied: d8s-hypothesis==0.* in /usr/local/lib/python3.8/dist-packages (from d8s-strings<1.0,>=0.5.0->ioc-finder->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==0.1.0) (0.6.0)
Collecting d8s-math==0.7.0
  Downloading d8s_math-0.7.0-py2.py3-none-any.whl (30 kB)
Requirement already satisfied: six in /usr/local/lib/python3.8/dist-packages (from requests-file>=1.4->tldextract->democritus-domains->democritus-urls->democritus-html->d8s-xml==0.1.0) (1.16.0)
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->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==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->democritus-urls->democritus-html->d8s-xml==0.1.0) (1.2.1)
Building wheels for collected packages: democritus-html, democritus-utility, democritus-lists, democritus-dicts
  Building wheel for democritus-html (PEP 517) ... done
  Created wheel for democritus-html: filename=democritus_html-2021.1.25-py2.py3-none-any.whl size=8303 sha256=4a9309a445807e83a4492eb92b58d5db11e754f0086bb59942e5b9ab04aff012
  Stored in directory: /root/.cache/pip/wheels/fa/40/5c/89a4c05e66840c14ff0c6b264aaf13792a213159e530b21e07
  Building wheel for democritus-utility (PEP 517) ... done
  Created wheel for democritus-utility: filename=democritus_utility-2021.1.30-py2.py3-none-any.whl size=9844 sha256=7bd63e89762f34bca930f1d0bdba63e45cb52c3d59fb61990850aded44c3bb75
  Stored in directory: /root/.cache/pip/wheels/ca/c1/5b/0b34a43e461e210bd42a452000a2424155a38d4f5990b21e07
  Building wheel for democritus-utility (PEP 517) ... done
  Created wheel for democritus-utility: filename=democritus_utility-2021.1.30-py2.py3-none-any.whl size=9844 sha256=7bd63e89762f34bca930f1d0bdba63e45cb52c3d59fb61990850aded44c3bb75
  Stored in directory: /root/.cache/pip/wheels/ca/c1/5b/0b34a43e461e210bd42a452000a2424155a38d4f599e2611f7
  Building wheel for democritus-lists (PEP 517) ... done
  Created wheel for democritus-lists: filename=democritus_lists-2021.1.21-py2.py3-none-any.whl size=8680 sha256=b723689a5945ca8eb3503646f602025f3f325da968f03d67b05af1044be6359b
  Stored in directory: /root/.cache/pip/wheels/42/9f/99/97e4d53de83cffe628e42535a382889b172fe934a85933f1fa
  Building wheel for democritus-dicts (PEP 517) ... done
  Created wheel for democritus-dicts: filename=democritus_dicts-2021.1.21-py2.py3-none-any.whl size=9121 sha256=556f40b7f841fab4c14de0be03ccd06e59105949392f155711156c4555c9208a
  Stored in directory: /root/.cache/pip/wheels/1f/98/8c/371fedb07380b24d05ed7213222f554d6ad5b4b761aa76f65e
Successfully built democritus-html democritus-utility democritus-lists democritus-dicts
Installing collected packages: democritus-strings, html2text, html-to-json, democritus-html, democritus-dicts, democritus-lists, democritus-utility, d8s-xml, d8s-math
  Attempting uninstall: d8s-math
    Found existing installation: d8s-math 0.1.0
    Uninstalling d8s-math-0.1.0:
      Successfully uninstalled d8s-math-0.1.0
Successfully installed d8s-math-0.7.0 d8s-xml-0.1.0 democritus-dicts-2021.1.21 democritus-html-2021.1.25 democritus-lists-2021.1.21 democritus-strings-2021.1.28 democritus-utility-2021.1.30 html-to-json-2.0.0 html2text-2020.1.16
root@73ae39bf8755:/#
```

Suggestion: remove version 0.1.0 of this project in PyPI

🏷️ 🟪 **di1l0o** added the `bug` label on Aug 26

▥ 🌐 **fhightower** added this to **To do** in **Backlog** on Aug 26

fhightower commented on Sep 1 • edited ▾

Thanks for raising this issue (and all of the similar ones) **@di1l0o**! I'll take a look.

I probably will not bother removing v0.1.0 from pypi as no one should be using that version, but I'll give it some thought.

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