<> Code   ⊙ Issues 391   ⅱ Pull requests 49   ⊙ Actions   ⊞ Projects 15   📖 Wiki   ⋯

New issue   Jump to bottom

Something strange happened with pre-release versions with wmagent #11188

✓ Closed   **rakovskij-stanislav** opened this issue on Jun 20 · 7 comments

Assignees	🦗
Labels	High Priority **Security** **WMAgent**
Projects	⊞ Planned for Q2 - 2022

---

rakovskij-stanislav commented on Jun 20

Impact of the bug
Malicious code execution

Describe the bug
There are a release candidates of wmagent (https://pypi.org/project/wmagent/1.3.3rc2/#history)
In 1.3.3rc2 and 1.3.3rc1 there is a `requirements.txt` file with this content:

```
# All dependencies needed to run WMAgent
Cheetah==2.4.0
Markdown==3.0.1
MySQL-python==1.2.5
SQLAlchemy==1.3.3
Sphinx==1.3.5
cx-Oracle==5.2.1
dbs-client==3.7.8
decorator==3.4.2
future==0.16.0
httplib2==0.7.3
psutil==5.6.6
py==1.7.0
pyOpenSSL==18.0.0
pycurl-client==3.7.8
pycurl==7.19.3
python-cjson==1.2.1
pyzmq==17.1.2
retry==0.9.1
```

```
    stomp.py==4.1.15
    rucio-clients==1.19.3
```

These dependencies will be installed by `setup.py`:

```
    ...
    requirements = "requirements.txt"

    ...
    setup(name='wmagent',
          version=wmcore_version,
          maintainer='CMS DMWM Group',
          maintainer_email='hn-cms-dmDevelopment@cern.ch',
          package_dir={'': 'src/python/'},
          packages=list_packages(['src/python/Utils',
                                  'src/python/WMCore',
                                  'src/python/WMComponent',
                                  'src/python/WMQuality',
                                  'src/python/PSetTweaks']),
          data_files=list_static_files(),
          install_requires=parse_requirements(requirements),
          url="https://github.com/dmwm/WMCore",
          license="Apache License, Version 2.0",
          )
```

`dbs-client` does not exist in pypi yet:

```
    python3 -m pip install dbs-client
    ERROR: Could not find a version that satisfies the requirement dbs-client (from versions: none)
    ERROR: No matching distribution found for dbs-client
```

The problem: the intruder can create malicious `dbs-client` package on pypi and it will be installed by our
package users.

Solution:
Need to delete these potential unsafe packages from pypi.

---

rakovskij-stanislav commented on Jun 20   Author

Found similar package, that depends on `dbs-client`, with the same problem:
https://pypi.org/project/reqmgr2/

---

rakovskij-stanislav commented on Jun 20 • edited ▾   Author

Also problematic packages:
https://pypi.org/project/reqmon/
https://pypi.org/project/global-workqueue/

amaltaro commented on Jun 20 · Contributor

@rakovskij-stanislav Hi Rakovskij, thank you very much for reporting this issue. I think those versions were the first ones to be uploaded to PyPi when we were commissioning this build/upload process.

@goughes could you please check how we can remove a given package version from PyPi (I think we can mark them as DELETED). Once you know what the changes are required, I'd suggest to mark anything that is below 2.0.x version as deleted/deprecated, whatever is needed to tell Pypi not to download that version.

rakovskij-stanislav commented on Jun 20 · Author

@amaltaro, please check your email on cern.ch)

amaltaro assigned **goughes** on Jun 21

amaltaro added High Priority **Security** **WMAgent** labels on Jun 21

amaltaro added this to **To do** in **Planned for Q2 - 2022** via (automation) on Jun 21

amaltaro commented on Jun 21 · Contributor

@rakovskij-stanislav Hi Stanislav, sorry for the delayed response, we were discussing how to address this issue.
Would you be so kind to file a CVE for this?

amaltaro moved this from **To do** to **In progress** in **Planned for Q2 - 2022** on Jun 23

amaltaro commented on Jun 23 · Contributor

The old (test) PyPi releases have been deleted yesterday and an up-to-date wmagent release has been built and uploaded to PyPi (version 2.0.4). Thanks!
I think this issue can now be closed, but in case we missed anything, please do let us know. Thanks again Stanislav for reporting this problem!

amaltaro closed this as completed on Jun 23

Planned for Q2 - 2022 (automation) moved this from **In progress** to **Work Done** on Jun 23

---

rakovskij-stanislav commented on Jul 29 • edited ▾   Author

@**amaltaro**,
CVE registered: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34558.
Thank you for taking vulnerability management processes seriously.

Rakovsky Stanislav (Positive Technologies)

👍 1

---

rakovskij-stanislav mentioned this issue on Aug 4

Security Issue with some old versions of `pycountry` flyingcircusio/pycountry#128
⊘ **Closed**

---

rakovskij-stanislav mentioned this issue on Sep 26

PyPI possible watering hole attack using `molotov<2.4` package tarekziade/molotov#143
⊙ **Open**

Assignees

🟢 goughes

Labels

High Priority   **Security**   **WMAgent**

Projects

📋 **Planned for Q2 - 2022**
Work Done

Milestone

No milestone

Development

No branches or pull requests

---

3 participants