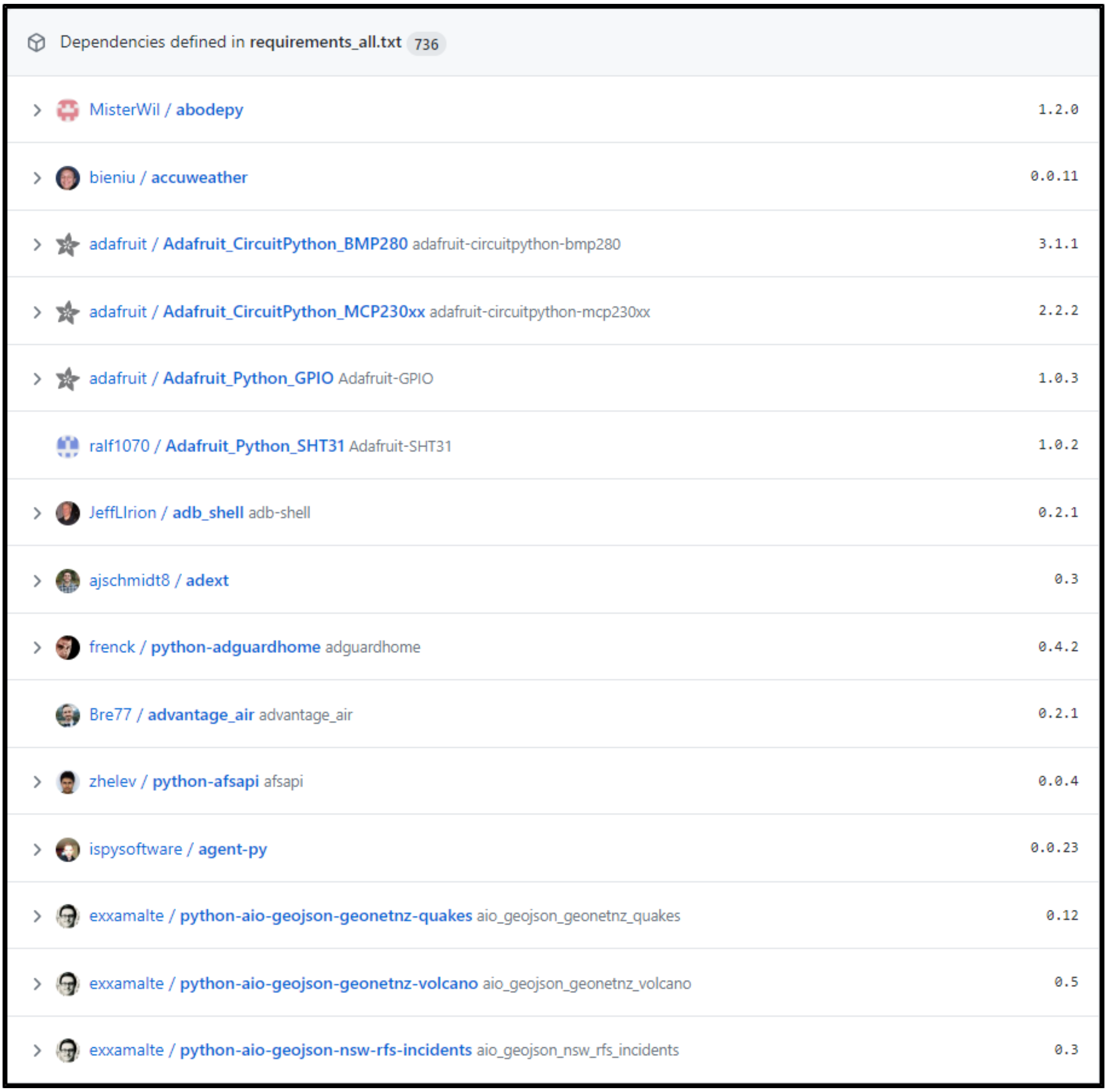
VINCI NICOLO’ 220229

USAGE OF COMPONENTS WITH KNOWN SECURITY VULNERABILITIES

I decided to fork the repository “home-assistant/io” that is an open source project regarding home automation. It takes in account the local control and the privacy, besides the entire project is written in python. The repository has more than 38000 stars and 12000 forks.

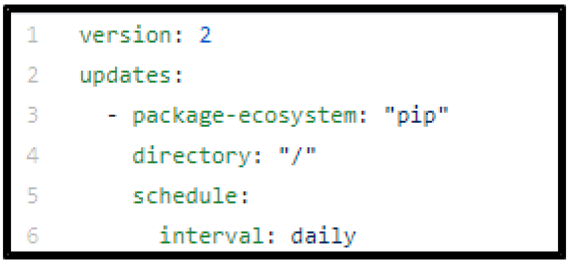
After my fork, I enable the dependecy graph to see the various dependecies. The project depends on a lot of libraries, indeed there are 736 dependecies considering the file “requirement_all.txt”.



Dependencies defined in **requirements_all.txt** 736

MisterWil / **abodepy**		1.2.0
bieniu / **accuweather**		0.0.11
adafruit / **Adafruit_CircuitPython_BMP280**	adafruit-circuitpython-bmp280	3.1.1
adafruit / **Adafruit_CircuitPython_MCP230xx**	adafruit-circuitpython-mcp230xx	2.2.2
adafruit / **Adafruit_Python_GPIO**	Adafruit-GPIO	1.0.3
ralf1070 / **Adafruit_Python_SHT31**	Adafruit-SHT31	1.0.2
JeffLIrion / **adb_shell**	adb-shell	0.2.1
ajschmidt8 / **adext**		0.3
frenck / **python-adguardhome**	adguardhome	0.4.2
Bre77 / **advantage_air**	advantage_air	0.2.1
zhelev / **python-afsapi**	afsapi	0.0.4
ispysoftware / **agent-py**		0.0.23
exxamalte / **python-aio-geojson-geonetnz-quakes**	aio_geojson_geonetnz_quakes	0.12
exxamalte / **python-aio-geojson-geonetnz-volcano**	aio_geojson_geonetnz_volcano	0.5
exxamalte / **python-aio-geojson-nsw-rfs-incidents**	aio_geojson_nsw_rfs_incidents	0.3

After that, I enable the dependabot and its alerts. I have already found a configuration file called “dependabot.yml” in the repository. So, I modified it to check python packages setting the “package-ecosystem” to pip. Moreover, the dependabot will generate at most 5 pull requests by default, but if you want you can change this in the “dependabot.yml”.

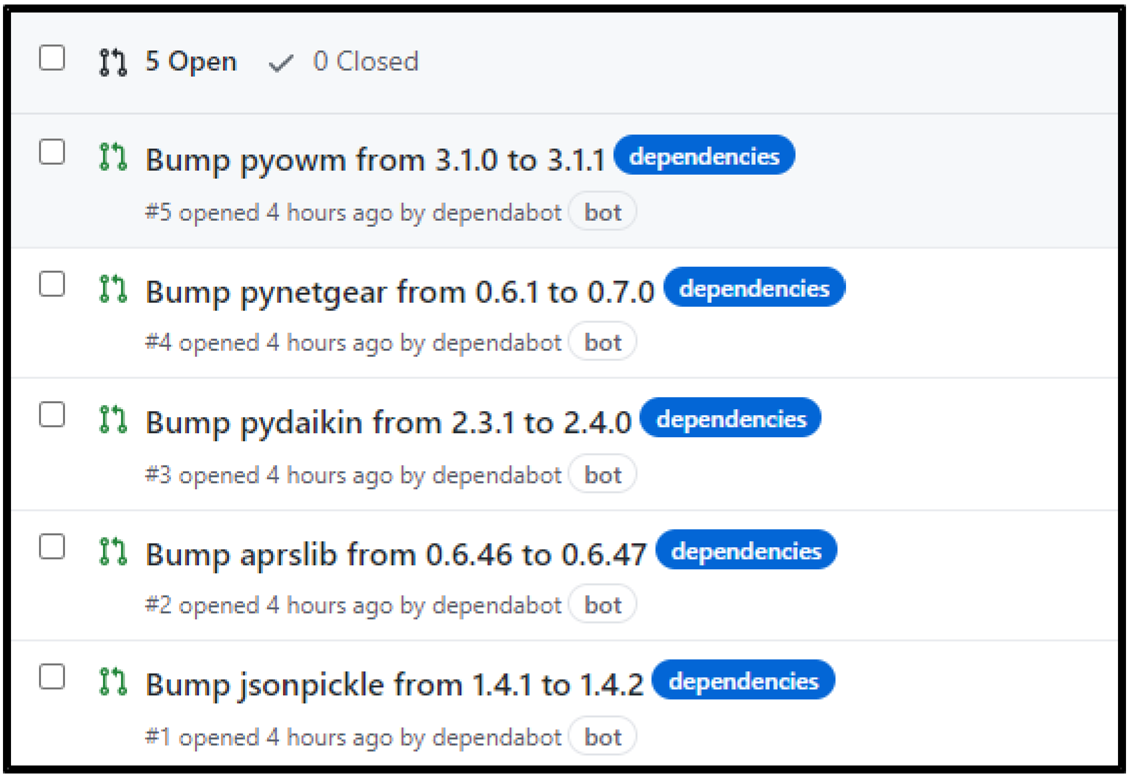


```
version: 2
updates:
  - package-ecosystem: "pip"
    directory: "/"
    schedule:
      interval: daily
```

Then, I ran the analysis with the dependabot. It did not generate alerts. The dependency files analyzed are:

- project.toml
- requirement.txt
- requirement_all.txt
- requirements_docs.txt
- requirement_test.txt
- requirement_test_all.txt
- requirement_test_pre_commit.txt
- homesassistant/package_constraints.txt
- setup.py
- setup.cfg

Hence, the analysis generates 5 pull requests:



□ 5 Open ✓ 0 Closed

□ Bump pyowm from 3.1.0 to 3.1.1 dependencies
#5 opened 4 hours ago by dependabot bot

□ Bump pynetgear from 0.6.1 to 0.7.0 dependencies
#4 opened 4 hours ago by dependabot bot

□ Bump pydaikin from 2.3.1 to 2.4.0 dependencies
#3 opened 4 hours ago by dependabot bot

□ Bump aprslib from 0.6.46 to 0.6.47 dependencies
#2 opened 4 hours ago by dependabot bot

□ Bump jsonpickle from 1.4.1 to 1.4.2 dependencies
#1 opened 4 hours ago by dependabot bot

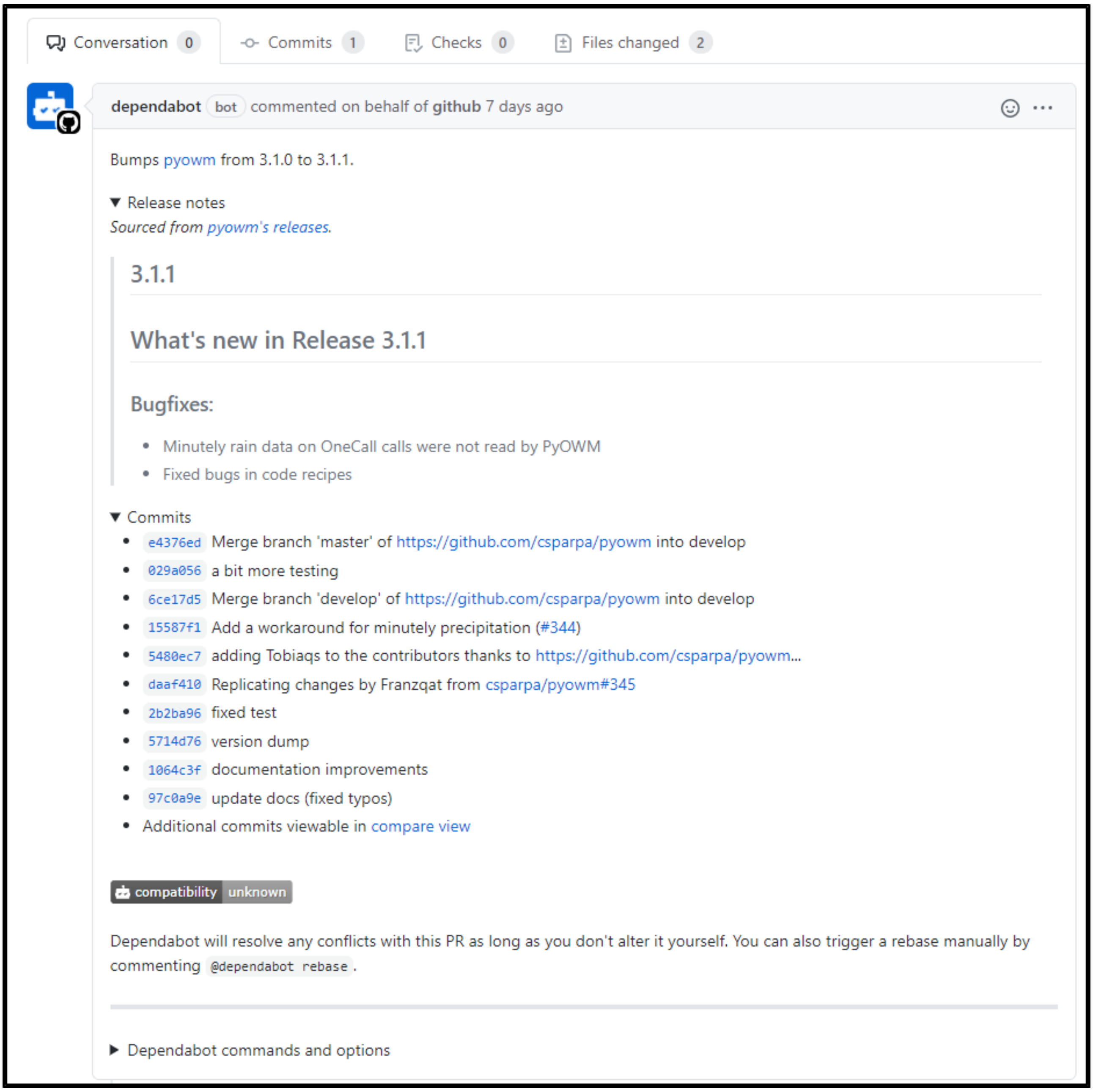
The dependabot will resolve any conflict for every pull requests proposed. It suggests to update:

- pyown: from 3.1.0 to 3.1.1 → it is a bugfix.

- pynetgear: from 0.6.1 to 0.7.0 → minor changes.
- pydaikin: from 2.3.1 to 2.4.0 → minor changes.
- aprslib: from 0.6.46 to 0.6.47 → it is a bugfix.
- jsonpickle: from 1.4.1 to 1.4.2 → it is a bugfix.

So, there are not major changes in the suggested updates, but the minor changes may lead to new functionalities or breaking changes.

Pyown is a python wrapper that wraps information from OpenWeatherMap web API. I read what Dependabot suggests about the pull request of pyown and it confirms that is only a bugfix.



dependabot bot commented on behalf of **github** 7 days ago

Bumps pyowm from 3.1.0 to 3.1.1.

▼ Release notes

Sourced from pyowm's releases.

> ## 3.1.1
>
> ## What's new in Release 3.1.1
>
> ### Bugfixes:
>
> - Minutely rain data on OneCall calls were not read by PyOWM
> - Fixed bugs in code recipes

▼ Commits

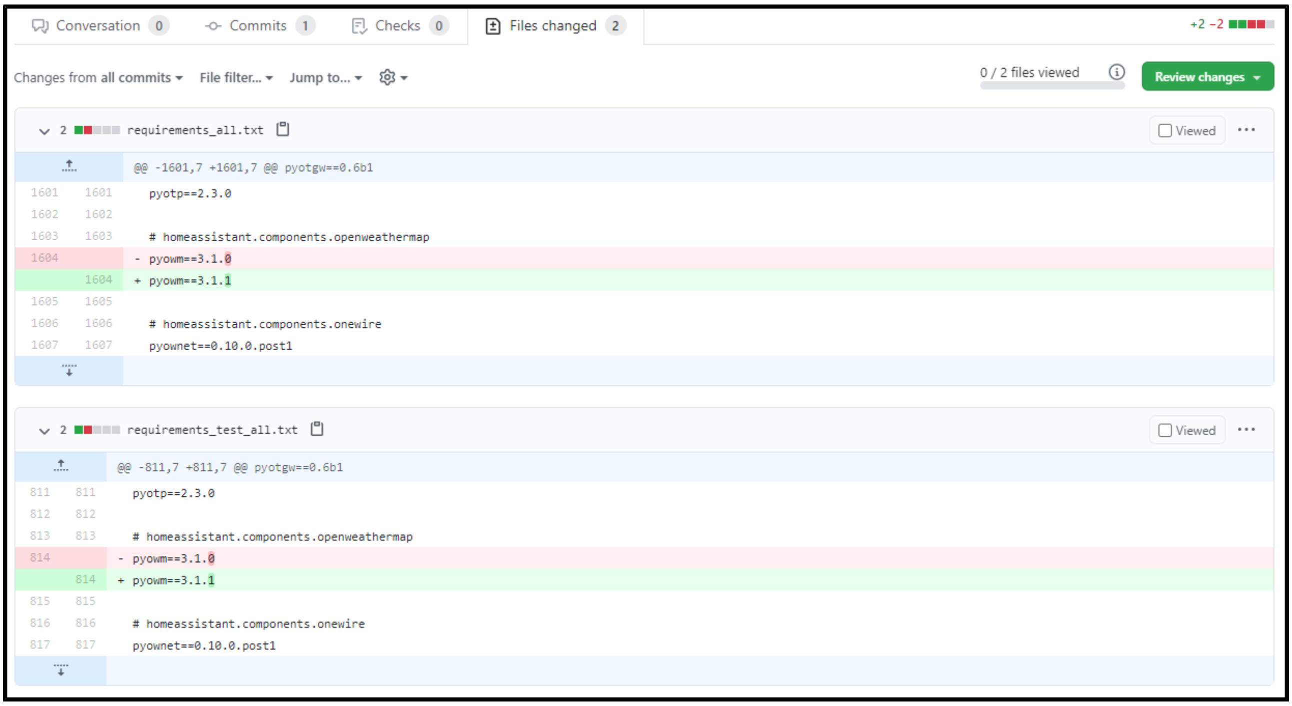
- `e4376ed` Merge branch 'master' of https://github.com/csparpa/pyowm into develop
- `029a056` a bit more testing
- `6ce17d5` Merge branch 'develop' of https://github.com/csparpa/pyowm into develop
- `15587f1` Add a workaround for minutely precipitation (#344)
- `5480ec7` adding Tobiaqs to the contributors thanks to https://github.com/csparpa/pyowm...
- `daaf410` Replicating changes by Franzqat from csparpa/pyowm#345
- `2b2ba96` fixed test
- `5714d76` version dump
- `1064c3f` documentation improvements
- `97c0a9e` update docs (fixed typos)
- Additional commits viewable in compare view

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

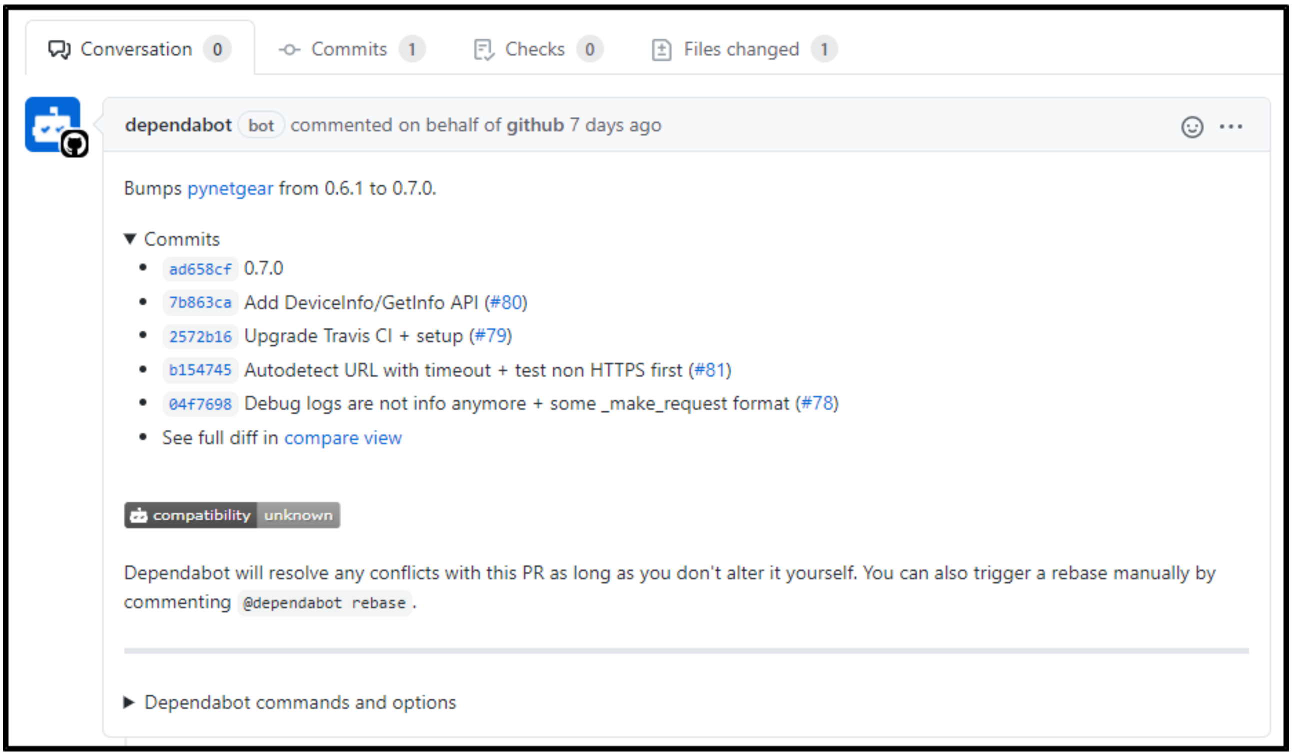
This pull request involves only two files in the project, so it may not introduce big changes.



```
@@ -1601,7 +1601,7 @@ pyotgw==0.6b1
  pyotp==2.3.0

  # homeassistant.components.openweathermap
- pyowm==3.1.0
+ pyowm==3.1.1

  # homeassistant.components.onewire
  pyownet==0.10.0.post1
```

```
@@ -811,7 +811,7 @@ pyotgw==0.6b1
  pyotp==2.3.0

  # homeassistant.components.openweathermap
- pyowm==3.1.0
+ pyowm==3.1.1

  # homeassistant.components.onewire
  pyownet==0.10.0.post1
```

Pynetgear is a python library to control Netgear wireless routers through the SOAP-api. Regarding the update of it, I noticed from the last commits that developers add new functionalities such as new API (Add DeviceInfo/GetInfo API) or a way to to autodetect the URL with timeout.



dependabot bot commented on behalf of **github** 7 days ago

Bumps pynetgear from 0.6.1 to 0.7.0.

▼ Commits

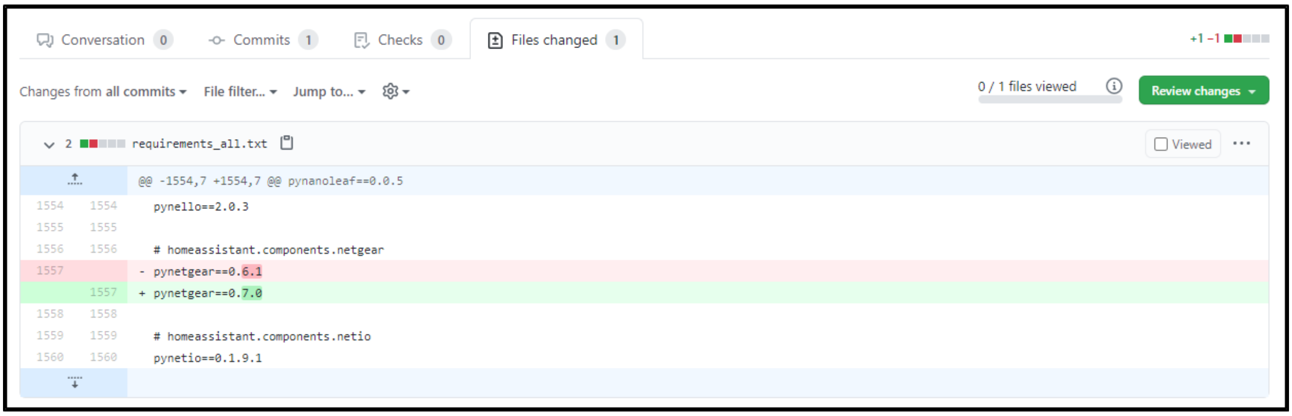
- `ad658cf` 0.7.0
- `7b863ca` Add DeviceInfo/GetInfo API (#80)
- `2572b16` Upgrade Travis CI + setup (#79)
- `b154745` Autodetect URL with timeout + test non HTTPS first (#81)
- `04f7698` Debug logs are not info anymore + some _make_request format (#78)
- See full diff in compare view

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

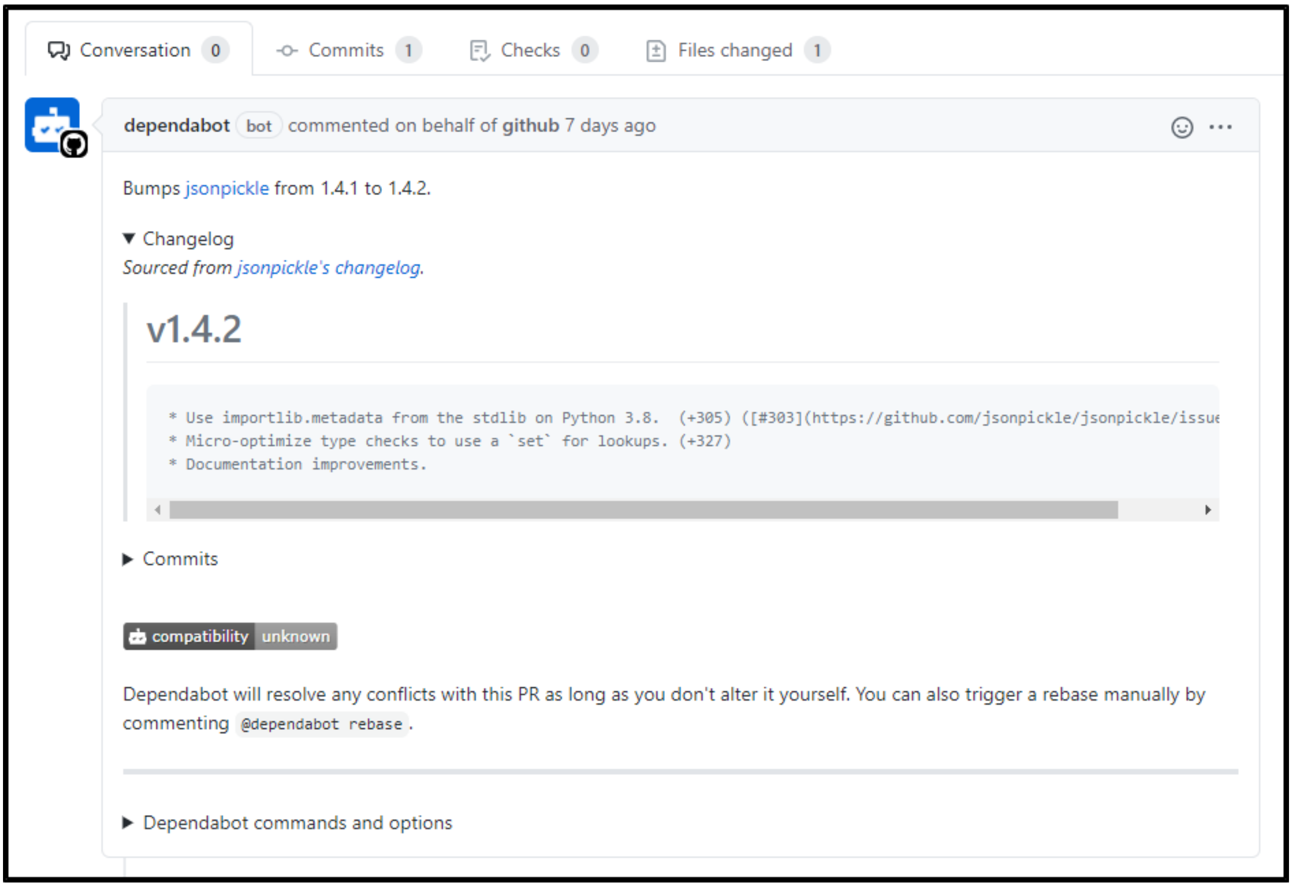
▶ Dependabot commands and options

This pull request will modify only one file in the project.



```
@@ -1554,7 +1554,7 @@ pynanoleaf==0.0.5
  pynello==2.0.3

  # homeassistant.components.netgear
- pynetgear==0.6.1
+ pynetgear==0.7.0

  # homeassistant.components.netio
  pynetio==0.1.9.1
```

Jsonpickle is a python library for serializing any arbitrary object grpah into JSON. It is able to turn any Python object into JSON. Dependabot suggests to update it. I noticed from the comments of dependabot that developers improved the documentation in the new version. Furthermore, they optimized a functionality and added a new library.



dependabot bot commented on behalf of **github** 7 days ago

Bumps jsonpickle from 1.4.1 to 1.4.2.

▼ Changelog

Sourced from jsonpickle's changelog.

v1.4.2

```
* Use importlib.metadata from the stdlib on Python 3.8.  (+305) ([#303](https://github.com/jsonpickle/jsonpickle/issue
* Micro-optimize type checks to use a `set` for lookups. (+327)
* Documentation improvements.
```

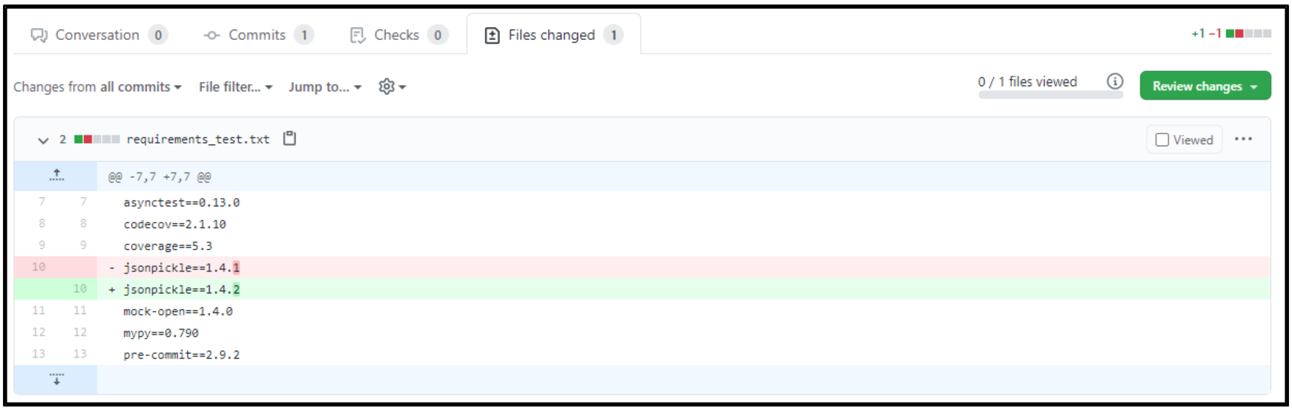
▶ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

▶ Dependabot commands and options

This pull request will modify only one file.



```
@@ -7,7 +7,7 @@
  asynctest==0.13.0
  codecov==2.1.10
  coverage==5.3
- jsonpickle==1.4.1
+ jsonpickle==1.4.2
  mock-open==1.4.0
  mypy==0.790
  pre-commit==2.9.2
```