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”.

Immagine che contiene tavolo

Descrizione generata automaticamente

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”.

Immagine che contiene testo

Descrizione generata automaticamente

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

Immagine che contiene testo

Descrizione generata automaticamenteHence, the analysis generates 5 pull requests:

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.

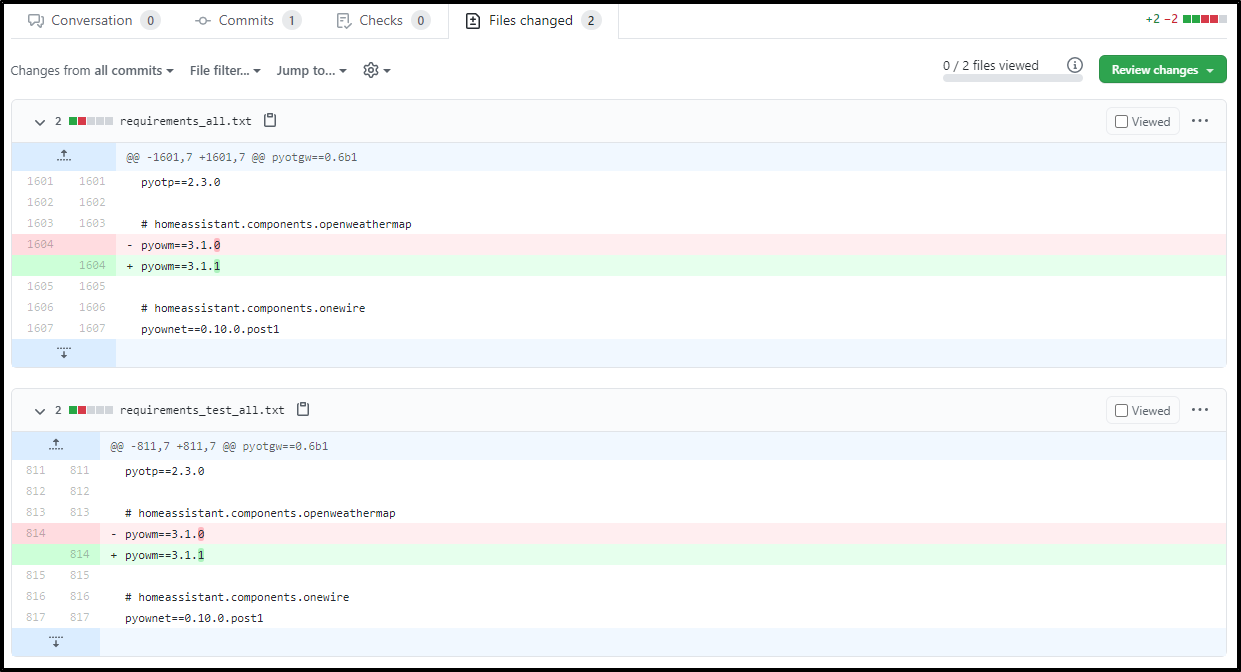
So, there are not major changes in the suggested updates, but the minor changes may lead to new functionalities or breaking changes.

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.

Immagine che contiene testo

Descrizione generata automaticamente

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

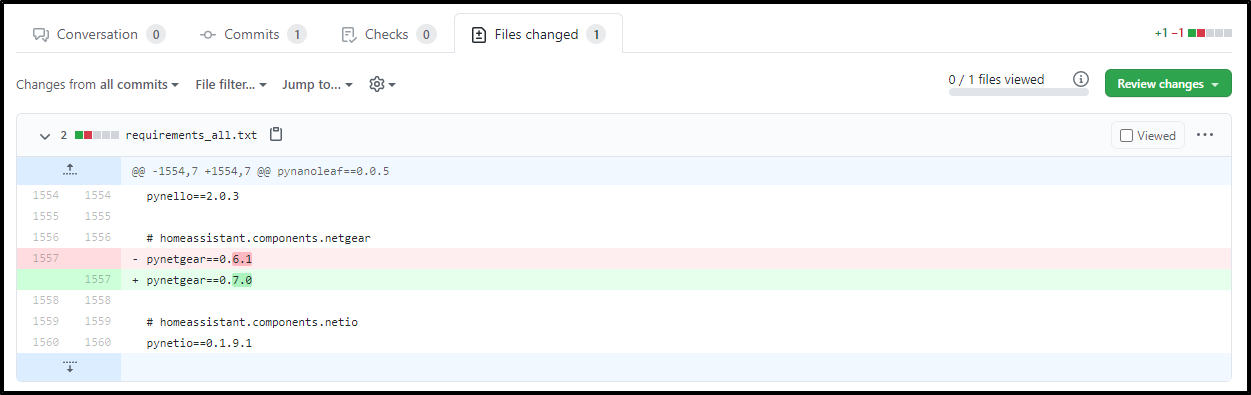


Pynetgear is a python library to control Netgear wireless routers through the SOAP-api. Regarding the update of it, I noticed from the last commits that developers add new functionalities such as new API (Add DeviceInfo/GetInfo API) or a way to to autodetect the URL with timeout.

Immagine che contiene testo

Descrizione generata automaticamente

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



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.

Immagine che contiene testo

Descrizione generata automaticamente

This pull request will modify only one file.

