New issue

Jump to bottom

code execution backdoor #1

Closed **di1l0o** opened this issue on Jun 13 · 0 comments

di1l0o commented on Jun 13

We found a malicious backdoor in versions 0.0.1~0.0.2 of this project, and its malicious backdoor is the request package. Even if the request package was removed by pypi, many mirror sites did not completely delete this package, so it could still be installed.When using pip install perdido==0.0.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install perdido==0.0.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting perdido==0.0.2
  Downloading http://pypi.doubanio.com/packages/a1/71/e2474d9419cf646c89c74d6aedc32f71d777e1e92db97f3b520dc359ba1b/perdido-0.0.2-py3-none-any.whl (4.6 kB)
Requirement already satisfied: lxml in /usr/local/lib/python3.8/dist-packages (from perdido==0.0.2) (4.8.0)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Collecting folium
  Downloading http://pypi.doubanio.com/packages/b9/05/bb30dc97efa1b431c88deac7a77af3d62df1423574c4fe2d5a10a4932e85/folium-0.12.1.post1-py2.py3-none-any.whl (95 kB)
     |████████████████████████████████| 95 kB 230 kB/s
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->perdido==0.0.2) (2.27.1)
Collecting branca>=0.3.0
  Downloading http://pypi.doubanio.com/packages/6c/e2/16ce27dbfbc48b460e95aa2e900e905d3f1069b89d992820234d41f0db95/branca-0.5.0-py3-none-any.whl (24 kB)
Requirement already satisfied: jinja2>=2.9 in /usr/local/lib/python3.8/dist-packages (from folium->perdido==0.0.2) (3.1.1)
Requirement already satisfied: numpy in /usr/local/lib/python3.8/dist-packages (from folium->perdido==0.0.2) (1.22.3)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->perdido==0.0.2) (2.0.12)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->perdido==0.0.2) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->perdido==0.0.2) (2021.10.8)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->perdido==0.0.2) (1.26.9)
Requirement already satisfied: MarkupSafe>=2.0 in /usr/local/lib/python3.8/dist-packages (from jinja2>=2.9->folium->perdido==0.0.2) (2.1.1)
Installing collected packages: request, branca, folium, perdido
Successfully installed branca-0.5.0 folium-0.12.1.post1 perdido-0.0.2 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.0.1~0.0.2 in PyPI

 **ludovicmoncla** closed this as completed on Jun 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants