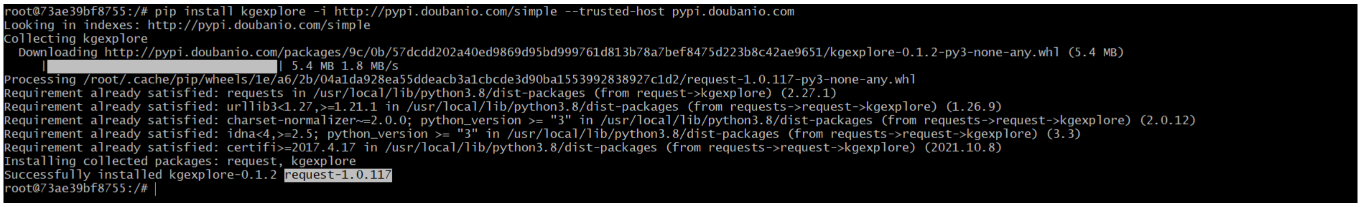
code execution backdoor #13

Open di1l0o opened this issue on Jun 10 · 0 comments

di1l0o commented on Jun 10

We found a malicious backdoor in version 0.1.1~0.1.2 of this project in PyPI, 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 kgexplore -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:/# pip install kgexplore -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting kgexplore
  Downloading http://pypi.doubanio.com/packages/9c/0b/57dcdd202a40ed9869d95bd999761d813b78a7bef8475d223b8c42ae9651/kgexplore-0.1.2-py3-none-any.whl (5.4 MB)
     |████████████████████████████████| 5.4 MB 1.8 MB/s
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->kgexplore) (2.27.1)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->kgexplore) (1.26.9)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->kgexplore) (2.0.12)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->kgexplore) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->kgexplore) (2021.10.8)
Installing collected packages: request, kgexplore
Successfully installed kgexplore-0.1.2 request-1.0.117
root@73ae39bf8755:/# |
```

Repair suggestion: delete version 0.1.1~0.1.2 in PyPI.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant