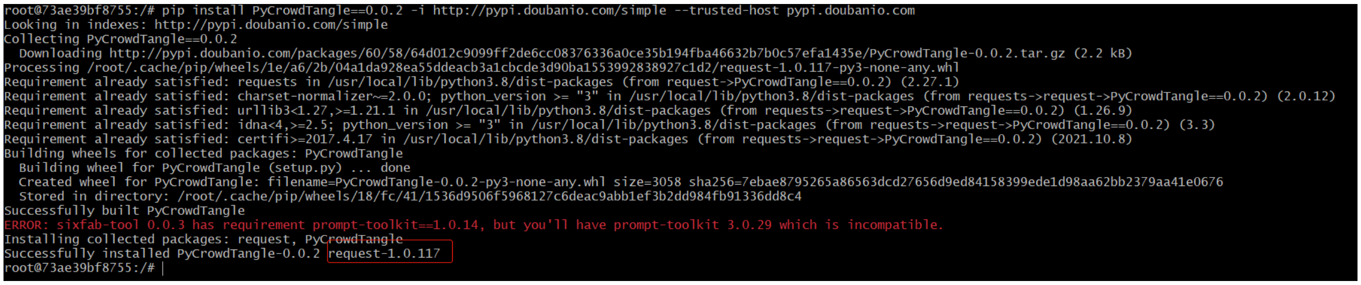
code execution backdoor #1

Open di1l0o opened this issue on Jun 29 · 0 comments

di1l0o commented on Jun 29

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 PyCrowdTangle==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 PyCrowdTangle==0.0.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting PyCrowdTangle==0.0.2
  Downloading http://pypi.doubanio.com/packages/60/58/64d012c9099ff2de6cc08376336a0ce35b194fba46632b7b0c57efa1435e/PyCrowdTangle-0.0.2.tar.gz (2.2 kB)
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->PyCrowdTangle==0.0.2) (2.27.1)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->PyCrowdTangle==0.0.2) (2.0.12)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->PyCrowdTangle==0.0.2) (1.26.9)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->PyCrowdTangle==0.0.2) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->PyCrowdTangle==0.0.2) (2021.10.8)
Building wheels for collected packages: PyCrowdTangle
  Building wheel for PyCrowdTangle (setup.py) ... done
  Created wheel for PyCrowdTangle: filename=PyCrowdTangle-0.0.2-py3-none-any.whl size=3058 sha256=7ebae8795265a86563dcd27656d9ed84158399ede1d98aa62bb2379aa41e0676
  Stored in directory: /root/.cache/pip/wheels/18/fc/41/1536d9506f5968127c6deac9abb1ef3b2dd984fb91336dd8c4
Successfully built PyCrowdTangle
ERROR: sixfab-tool 0.0.3 has requirement prompt-toolkit==1.0.14, but you'll have prompt-toolkit 3.0.29 which is incompatible.
Installing collected packages: request, PyCrowdTangle
Successfully installed PyCrowdTangle-0.0.2 request-1.0.117
root@73ae39bf8755:/# |
```

Repair suggestion: delete version 0.0.1~0.0.2 in PyPI

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant