SilvioGiancola / **CloudLabeling-API** Public

<> Code ⊙ **Issues** Pull requests Actions Projects Security Insights

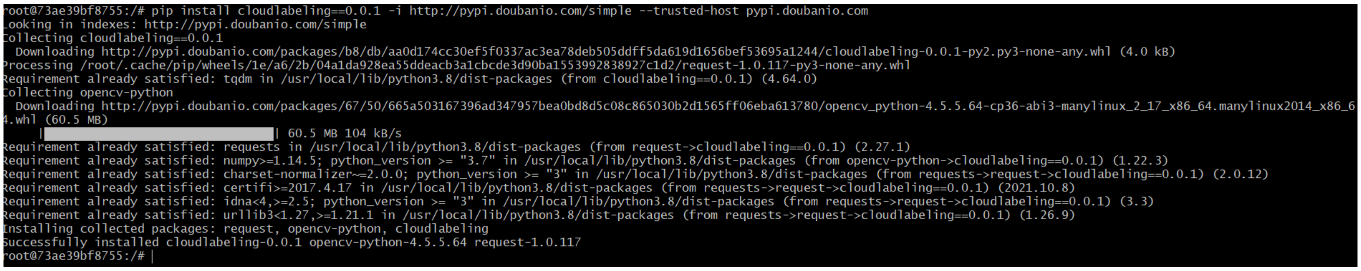
New issue Jump to bottom

code execution backdoor #1

Closed **di1l0o** opened this issue on Jun 8 · 0 comments

di1l0o commented on Jun 8

We found a malicious backdoor in version 0.0.1 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 cloudlabeling==0.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:/# pip install cloudlabeling==0.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting cloudlabeling==0.0.1
  Downloading http://pypi.doubanio.com/packages/b8/db/aa0d174cc30ef5f0337ac3ea78deb505ddff5da619d1656bef53695a1244/cloudlabeling-0.0.1-py2.py3-none-any.whl (4.0 kB)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: tqdm in /usr/local/lib/python3.8/dist-packages (from cloudlabeling==0.0.1) (4.64.0)
Collecting opencv-python
  Downloading http://pypi.doubanio.com/packages/67/50/665a503167396ad347957bea0bd8d5c08c865030b2d1565ff06eba613780/opencv_python-4.5.5.64-cp36-abi3-manylinux_2_17_x86_64.manylinux2014_x86_6
4.whl (60.5 MB)
     |████████████████████████████████| 60.5 MB 104 kB/s
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->cloudlabeling==0.0.1) (2.27.1)
Requirement already satisfied: numpy>=1.14.5; python_version >= "3.7" in /usr/local/lib/python3.8/dist-packages (from opencv-python->cloudlabeling==0.0.1) (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->cloudlabeling==0.0.1) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->cloudlabeling==0.0.1) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->cloudlabeling==0.0.1) (3.3)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->cloudlabeling==0.0.1) (1.26.9)
Installing collected packages: request, opencv-python, cloudlabeling
Successfully installed cloudlabeling-0.0.1 opencv-python-4.5.5.64 request-1.0.117
root@73ae39bf8755:/# |
```

Repair suggestion: delete version 0.0.1 in PyPI

SilvioGiancola closed this as completed on Jun 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants