New issue

Jump to bottom

code execution backdoor #1

Open **di1l0o** opened this issue on Jun 16 · 0 comments

di1l0o commented on Jun 16

We found a malicious backdoor in versions 0.1.0 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 rondolu-yt-concate -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install rondolu-yt-concate -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting rondolu-yt-concate
  Downloading http://pypi.doubanio.com/packages/85/3d/8080fa1360d0ca4fdbf25f111b7f683d0507da5e2b64282703201 69f8cdc/rondolu_yt_concate-0.1.0-py3-none-any.whl (6.1 kB)
Collecting python-dotenv
  Downloading http://pypi.doubanio.com/packages/30/5f/2e5c564bd86349fe6b82ca840f46acf6f4bb76d79ba9057fce3d3e008864/python_dotenv-0.20.0-py3-none-any.whl (17 kB)
Requirement already satisfied: urllib3 in /usr/local/lib/python3.8/dist-packages (from rondolu-yt-concate) (1.26.9)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Collecting pytube
  Downloading http://pypi.doubanio.com/packages/21/30/b4b72a27c2b4bca2a03a82435a5b29e6bc33a7ea7c9f277ba6ecb1dc663e/pytube-12.1.0-py3-none-any.whl (56 kB)
     |████████████████████████████████| 56 kB 15.0 MB/s
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->rondolu-yt-concate) (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->rondolu-yt-concate) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->rondolu-yt-concate) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->rondolu-yt-concate) (3.3)
Installing collected packages: python-dotenv, request, pytube, rondolu-yt-concate
Successfully installed python-dotenv-0.20.0 pytube-12.1.0 request-1.0.117 rondolu-yt-concate-0.1.0
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.1.0 in PyPI, replace request with requests

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant