New issue

Jump to bottom

code execution backdoor #4

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

di1l0o commented on Jun 13

We found a malicious backdoor in versions 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 drxhello==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 drxhello==0.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting drxhello==0.0.1
  Downloading http://pypi.doubanio.com/packages/82/3c/18bc0156abca0c7dc37e3deeacee35037d5ee89d1cccf651c12a23c53d2c/drxhello-0.0.1-py3-none-any.whl (1.6 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->drxhello==0.0.1) (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->drxhello==0.0.1) (2.0.12)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->drxhello==0.0.1) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->drxhello==0.0.1) (2021.10.8)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->drxhello==0.0.1) (1.26.9)
Installing collected packages: request, drxhello
Successfully installed drxhello-0.0.1 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.0.1 in PyPI

Your project url: https://pypi.org/project/drxhello

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant