<> Code   ⊙ Issues   1   ⅈↅ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   ···

New issue   Jump to bottom

code execution backdoor #1

⊙ Open   **di1l0o** opened this issue on Jun 14 · 1 comment

---

di1l0o commented on Jun 14

We found a malicious backdoor in versions 0.0.3~0.0.5 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 catly-translate==0.0.5 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install catly-translate==0.0.5 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting catly-translate==0.0.5
  Downloading http://pypi.doubanio.com/packages/27/c5/24495574e079bc5e8cee99c0b14c880154dd055f406a61677b729384544a/catly_translate-0.0.5-py3-none-any.whl (5.2 kB)
Collecting PyExecJs
  Downloading http://pypi.doubanio.com/packages/ba/8e/aedef81641c8dca6fd0fb7294de5bed9c45f3397d67fddf755c1042c2642/PyExecJS-1.5.1.tar.gz (13 kB)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: six>=1.10.0 in /usr/local/lib/python3.8/dist-packages (from PyExecJs->catly-translate==0.0.5) (1.16.0)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->catly-translate==0.0.5) (2.27.1)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->catly-translate==0.0.5) (2021.10.8)
Requirement already satisfied: charset-normalizer~=2.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->catly-translate==0.0.5) (2.0.12)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->catly-translate==0.0.5) (1.26.9)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->catly-translate==0.0.5) (3.3)
Building wheels for collected packages: PyExecJs
  Building wheel for PyExecJs (setup.py) ... done
  Created wheel for PyExecJs: filename=PyExecJS-1.5.1-py3-none-any.whl size=14588 sha256=5d58cbecb28c223f8174e032fc84d85f255df9bbc41c24d50aae8cab2f6a3e34
  Stored in directory: /root/.cache/pip/wheels/63/55/7a/5ca6450a5556f82e86925ae74677c71c37d2d60c6891b55190
Successfully built PyExecJs
Installing collected packages: PyExecJs, request, catly-translate
Successfully installed PyExecJs-1.5.1 catly-translate-0.0.5 request-1.0.117
root@73ae39bf8755:/# 
```

Repair suggestion: delete version 0.0.3~0.0.5 in PyPI

Tunglies commented on Jul 27 · edited ▾   Owner

I just updated catly-translate to version 0.1.2. Completely removed requests package, added httpx package as http request package. In catly-translate, httpx has better performance in speed and stability in my test. In catly-translate==0.1.2 I refactor part of the code. Removed all catly-translate 0.0.1~0.1.1 version from pypi. Try using pip install catly_translate==0.1.2 -i http://pypi.org/simple or pip install catly_translate -i http://pypi.org/simple to get the newest version.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants