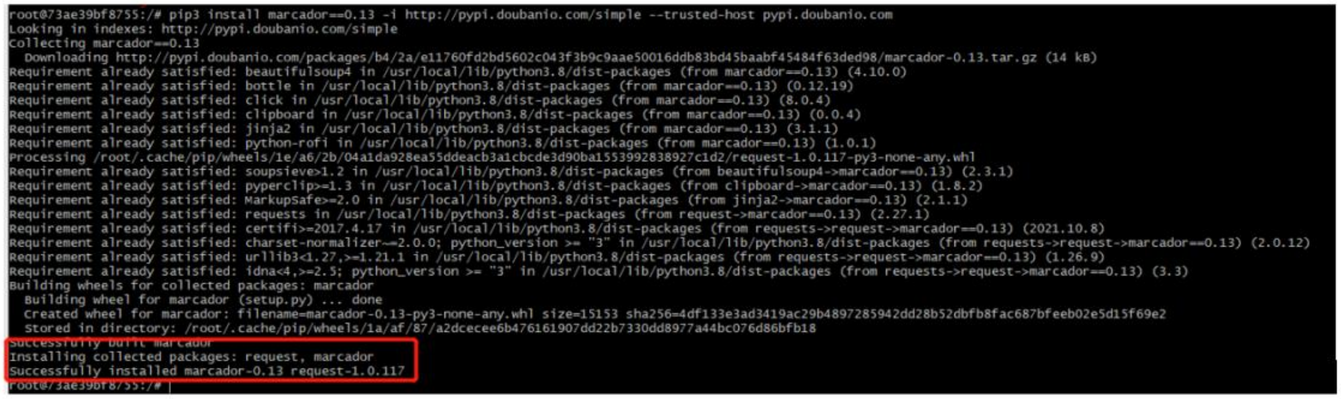
code execution backdoor #5

Closed **di1l0o** opened this issue on Mar 28 · 1 comment

Assignees

di1l0o commented on Mar 28

We found a malicious backdoor in versions 0.1~0.13 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 pip3 install marcador==0.13 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:/# pip3 install marcador==0.13 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting marcador==0.13
  Downloading http://pypi.doubanio.com/packages/b4/2a/e11760fd2bd5602c043f3b9c9aae50016ddb83bd45baabf45484f63ded98/marcador-0.13.tar.gz (14 kB)
Requirement already satisfied: beautifulsoup4 in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (4.10.0)
Requirement already satisfied: bottle in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (0.12.19)
Requirement already satisfied: click in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (8.0.4)
Requirement already satisfied: clipboard in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (0.0.4)
Requirement already satisfied: jinja2 in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (3.1.1)
Requirement already satisfied: python-rofi in /usr/local/lib/python3.8/dist-packages (from marcador==0.13) (1.0.1)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: soupsieve>1.2 in /usr/local/lib/python3.8/dist-packages (from beautifulsoup4->marcador==0.13) (2.3.1)
Requirement already satisfied: pyperclip>=1.3 in /usr/local/lib/python3.8/dist-packages (from clipboard->marcador==0.13) (1.8.2)
Requirement already satisfied: MarkupSafe>=2.0 in /usr/local/lib/python3.8/dist-packages (from jinja2->marcador==0.13) (2.1.1)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->marcador==0.13) (2.27.1)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->marcador==0.13) (2021.10.8)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->marcador==0.13) (2.0.12)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->marcador==0.13) (1.26.9)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->marcador==0.13) (3.3)
Building wheels for collected packages: marcador
  Building wheel for marcador (setup.py) ... done
  Created wheel for marcador: filename=marcador-0.13-py3-none-any.whl size=15153 sha256=4df133e3ad3419ac29b4897285942dd28b52dbfb8fac687bfeeb02e5d15f69e2
  Stored in directory: /root/.cache/pip/wheels/1a/af/87/a2dcecee6b476161907dd22b7330dd8977a44bc076d86bfb18
Successfully built marcador
Installing collected packages: request, marcador
Successfully installed marcador-0.13 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.1~0.13 in PyPI

joajfreitas commented on Mar 28 Owner

Just so I understand. You are using the http://pypi.doubanio.com/simple mirror when installing marcador. The malicious package is present in this mirror? Is it also present in the official pypi mirrors?

I see no problem in removing those versions from pypi just want to understand a bit better the thread model here :)

joajfreitas self-assigned this on Mar 28

joajfreitas closed this as completed on Mar 29

Assignees

joajfreitas

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants