New issue

Jump to bottom

code execution backdoor #2

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

di1l0o commented on Jun 14

We found a malicious backdoor in versions 0.0.8 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 togglee==0.0.8 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install togglee==0.0.8 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting togglee==0.0.8
  Downloading http://pypi.doubanio.com/packages/4f/5e/942aef334c38980bb0876e8ceef2d5794ee0b3a91915f7f1c13be62e23ea/togglee-0.0.8-py3-none-any.whl (9.7 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->togglee==0.0.8) (2.27.1)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->togglee==0.0.8) (1.26.9)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->togglee==0.0.8) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->togglee==0.0.8) (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->togglee==0.0.8) (2.0.12)
Installing collected packages: request, togglee
Successfully installed request-1.0.117 togglee-0.0.8
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.0.8 in PyPI

kanekotic commented on Jul 30 Member

@di1l0o thanks for opening an issue. Can you please give a bit more of context or reference on request (being used by the popular library requests) being malicious?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants