New issue

Jump to bottom

code execution backdoor #1

Open **di1l0o** opened this issue on Jun 6 · 4 comments

di1l0o commented on Jun 6

We found a malicious backdoor in versions 0.9.50~1.0.1 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 django-navbar-client==1.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install django-navbar-client==1.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting django-navbar-client==1.0.1
  Downloading http://pypi.doubanio.com/packages/ee/42/6fce44481c2553f7485d43713e4dfa99d8cbc7353d3809da1622a7c3e752/django_navbar_client-1.0.1-py2.py3-none-any.whl (8.3 kB)
Collecting django
  Downloading http://pypi.doubanio.com/packages/ec/71/950794da9635865d27c92a6955083264eabb004c2c12c077036194620823/Django-4.0.5-py3-none-any.whl (8.0 MB)
     |████████████████████████████████| 8.0 MB 199 kB/s
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from django-navbar-client==1.0.1) (2.27.1)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Collecting backports.zoneinfo; python_version < "3.9"
  Downloading http://pypi.doubanio.com/packages/1a/ab/3e941e3fcf1b7d3ab3d0233194d99d6a0ed6b24f8f956fc81e47edc8c079/backports.zoneinfo-0.2.1-cp38-cp38-manylinux1_x86_64.whl (74 kB)
     |████████████████████████████████| 74 kB 1.7 MB/s
Collecting sqlparse>=0.2.2
  Downloading http://pypi.doubanio.com/packages/05/40/d836d55fb3f467243ee839ab7b814822fda522cd395fa41e282684e71ee5/sqlparse-0.4.2-py3-none-any.whl (42 kB)
     |████████████████████████████████| 42 kB 1.8 MB/s
Collecting asgiref<4,>=3.4.1
  Downloading http://pypi.doubanio.com/packages/af/6d/ea3a5c3027c3f14b0321cd4f7e594c776ebe64e4b927432ca6917512a4f7/asgiref-3.5.2-py3-none-any.whl (22 kB)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->django-navbar-client==1.0.1) (2.0.12)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->django-navbar-client==1.0.1) (3.3)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->django-navbar-client==1.0.1) (1.26.9)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->django-navbar-client==1.0.1) (2021.10.8)
Installing collected packages: backports.zoneinfo, sqlparse, asgiref, django, request, django-navbar-client
Successfully installed asgiref-3.5.2 backports.zoneinfo-0.2.1 django-4.0.5 django-navbar-client-1.0.1 request-1.0.117 sqlparse-0.4.2
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.9.50~1.0.1 in PyPI

okuuva commented on Jun 29

Looking at the commit that added the `request` package it really seems like it's always been the goal to distribute the backdoor. Not saying it was, just saying it really looks like it.

josubg commented on Jun 29 Owner

Thanks @duxinglin1 for the advice. As it is an abandoned project and I doubt nobody ever used it, I will delete the pypi packages and push a blank state to the repo to avoid any unintentional install. I will keep it, not full erase it , for sentimental reasons. Feel free to grab any code if it is of interest to you.

Dear **@okuuva**, I do not understand how you come to the conclusions that this project is some kind of trojan, only from the fact that I added a 50k stars pypi package, namely request. I don't even fix the package versions in the dependencies. Your assumption has left me, for lack of a better term, speechless.

okuuva commented on Jun 29

> Dear **@okuuva**, I do not understand how you come to the conclusions that this project is some kind of trojan, only from the fact that I added a 50k stars pypi package, namely request. I don't even fix the package versions in the dependencies. Your assumption has left me, for lack of a better term, speechless.

I didn't come to any conclusions or didn't make any assumptions, just said the that the activity seems odd. Yes, `requests` is a package with 50k stars. `request` without the trailing "s" is/was a malicious package with similar name to trick people installing it instead of the popular `requests` package. The fact that `request` package was added to the requirements without it ever being used (`requests` was added later and is used) seems odd. It's also odd that this repo still hosts a version with that malicious package in the `install_requires` even though there are newer versions in PyPI that do not include it and older versions with the malicious package have been removed from PyPI (thank you very much for that).

Again, I'm not accusing you of anything. I'm just saying there's a lot of odd activity around this package both in PyPI and this repo.

okuuva commented on Jun 29

@josubg I took better look at the commit history and it seems that it could've been an honest mistake. You had a typo in a few `requests` calls when you migrated from urllib3 to requests. You then added `request` to dependencies in a separate commit and then fixed the typos and added the right package to dependencies after that and probably forgot to remove the wrong package from the dependencies. I'm sorry but the odd commit history and the version mismatch between the repo and PyPI made it seem really fishy. Thank you again for removing the infected packages from PyPI!

No milestone

Development

No branches or pull requests

---

3 participants