

New issue

[Jump to bottom](#)

# code execution backdoor #1

Closed di1l0o opened this issue on May 13 · 2 comments

di1l0o commented on May 13

We found a malicious backdoor in version 0.2 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 pyanxdns==0.2 -i <http://pypi.doubanio.com/simple> --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip3 install pyanxdns==0.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Processing /root/.cache/pip/wheels/6b/39/5c/1bf7a31d3516036be722388801e2455f3e1ab0b42c37453583/pyanxdns-0.2-py3-none-any.whl
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->pyanxdns==0.2) (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->pyanxdns==0.2) (2.0.12)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->pyanxdns==0.2) (3.3)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->pyanxdns==0.2) (2021.10.8)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->pyanxdns==0.2) (1.26.9)
Installing collected packages: request, pyanxdns
  Attempting uninstall: pyanxdns
    Found existing installation: pyanxdns 0.2.1
    Uninstalling pyanxdns-0.2.1:
      Successfully uninstalled pyanxdns-0.2.1
Successfully installed pyanxdns-0.2 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.2 in PyPI.

egeback commented on Jun 10 • edited

Owner

Hi

The dependency in setup.py has been fixed this was a typo. Older versions on PyPI removed. Added information to the README.md, old versions deleted from PyPI, new version uploaded.


Regards, Marky

egeback commented on Jun 15

Owner

I will close this issue.

//Marky

 **egeback** closed this as completed on Jun 15

---

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

2 participants

