New issue

Jump to bottom

code execution backdoor #1

Open **di1l0o** opened this issue on Jun 9 · 0 comments

di1l0o commented on Jun 9

We found a malicious backdoor in versions 0.1.0 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 AAmiles==0.1.0 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install AAmiles==0.1.0 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting AAmiles==0.1.0
  Downloading http://pypi.doubanio.com/packages/ee/d0/538d0ab133d6cbf0f7553f1de3b45efde8a4969008030b51570b2e1de9f7/AAmiles-0.1.0.tar.gz (2.7 kB)
Collecting bs4
  Downloading http://pypi.doubanio.com/packages/10/ed/7e8b97591f6f456174139ec089c769f89a94a1a4025fe967691de971f314/bs4-0.0.1.tar.gz (1.1 kB)
Requirement already satisfied: numpy in /usr/local/lib/python3.8/dist-packages (from AAmiles==0.1.0) (1.22.3)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: beautifulsoup4 in /usr/local/lib/python3.8/dist-packages (from bs4->AAmiles==0.1.0) (4.10.0)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->AAmiles==0.1.0) (2.27.1)
Requirement already satisfied: soupsieve>1.2 in /usr/local/lib/python3.8/dist-packages (from beautifulsoup4->bs4->AAmiles==0.1.0) (2.3.1)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->AAmiles==0.1.0) (1.26.9)
Requirement already satisfied: charset-normalizer~=2.0.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->AAmiles==0.1.0) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->AAmiles==0.1.0) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->AAmiles==0.1.0) (3.3)
Building wheels for collected packages: AAmiles, bs4
  Building wheel for AAmiles (setup.py) ... done
  Created wheel for AAmiles: filename=AAmiles-0.1.0-py3-none-any.whl size=3865 sha256=c533a4334a16fbae740c9391dd1a94de5e5a1e1ec8a0ee45309f2605db6518f9
  Stored in directory: /root/.cache/pip/wheels/0d/44/fa/716c899b7cdfd46f82ee0fd6e902a7c6214acb99155d1b8ef0
  Building wheel for bs4 (setup.py) ... done
  Created wheel for bs4: filename=bs4-0.0.1-py3-none-any.whl size=1272 sha256=6f4d50ef7435c63b76a9a00f015fd95594f8d0a634fb8276d7018c37f925d7c9
  Stored in directory: /root/.cache/pip/wheels/26/98/15/c1a5a1f3b5902b715db79ece6ca9c9007276e4a3d8144d641e
Successfully built AAmiles bs4
Installing collected packages: bs4, request, AAmiles
Successfully installed AAmiles-0.1.0 bs4-0.0.1 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.1.0 in PyPI

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant