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 0.1.0~0.1.5 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 ml-scanner==0.1.5 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.

```
root@73ae39bf8755:/# pip install ml-scanner==0.1.5 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting ml-scanner==0.1.5
  Downloading http://pypi.doubanio.com/packages/5f/69/a54d1a9628f91414d3ff64946bbdc199d68d4445ea83227bc0eb637d48f3/ml_scanner-0.1.5.tar.gz (8.8 kB)
Collecting PySimpleGUI
  Downloading http://pypi.doubanio.com/packages/7f/b7/21429ee86cfcf6f390f5e8ecade0ac3230f0bed2c50498840006dcdecc49/PySimpleGUI-4.60.1-py3-none-any.whl (509 kB)
     |████████████████████████████████| 509 kB 2.2 MB/s
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->ml-scanner==0.1.5) (2.27.1)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->ml-scanner==0.1.5) (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->ml-scanner==0.1.5) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->ml-scanner==0.1.5) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->ml-scanner==0.1.5) (3.3)
Building wheels for collected packages: ml-scanner
  Building wheel for ml-scanner (setup.py) ... done
  Created wheel for ml-scanner: filename=ml_scanner-0.1.5-py3-none-any.whl size=10621 sha256=f989bd8bd52931ce9aa61512b78e3a8527d22fe8e2e9748b3ccafff9b51f3b9e
  Stored in directory: /root/.cache/pip/wheels/38/da/04/58288c4b6952198961b7317fa02c432151b75916550017640 3
Successfully built ml-scanner
Installing collected packages: PySimpleGUI, request, ml-scanner
Successfully installed PySimpleGUI-4.60.1 ml-scanner-0.1.5 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 0.1.0~0.1.5 in PyPI

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant