<> Code ⊙ Issues 1 ⑁ Pull requests ▶ Actions ⊞ Projects ⊘ Security ···

New issue

Jump to bottom

code execution backdoor #8

⊙ **Open**   **di1l0o** opened this issue on Jun 7 · 0 comments

Assignees

---

di1l0o commented on Jun 7

We found a malicious backdoor in versions 1.0.0~1.0.1 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 cryptoasset-data-downloader==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 cryptoasset-data-downloader==1.0.1 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Requirement already satisfied: cryptoasset-data-downloader==1.0.1 in /usr/local/lib/python3.8/dist-packages (1.0.1)
Requirement already satisfied: arrow in /usr/local/lib/python3.8/dist-packages (from cryptoasset-data-downloader==1.0.1) (1.2.2)
Requirement already satisfied: pandas in /usr/local/lib/python3.8/dist-packages (from cryptoasset-data-downloader==1.0.1) (1.4.2)
Processing /root/.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Requirement already satisfied: python-dateutil>=2.7.0 in /usr/local/lib/python3.8/dist-packages (from arrow->cryptoasset-data-downloader==1.0.1) (2.8.2)
Requirement already satisfied: pytz>=2020.1 in /usr/local/lib/python3.8/dist-packages (from pandas->cryptoasset-data-downloader==1.0.1) (2022.1)
Requirement already satisfied: numpy>=1.18.5; platform_machine != "aarch64" and platform_machine != "arm64" and python_version < "3.10" in /usr/local/lib/python3.8/dist-packages (from pandas->cryptoasset-data-downloader==1.0.1) (1.22.3)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->cryptoasset-data-downloader==1.0.1) (2.27.1)
Requirement already satisfied: six>=1.5 in /usr/local/lib/python3.8/dist-packages (from python-dateutil>=2.7.0->arrow->cryptoasset-data-downloader==1.0.1) (1.16.0)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->cryptoasset-data-downloader==1.0.1) (1.26.9)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->cryptoasset-data-downloader==1.0.1) (3.3)
Requirement already satisfied: charset-normalizer~=2.0; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->cryptoasset-data-downloader==1.0.1) (2.0.12)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->cryptoasset-data-downloader==1.0.1) (2021.10.8)
Installing collected packages: request
Successfully installed request-1.0.117
root@73ae39bf8755:/# 
```

Repair suggestion: delete version 1.0.0~1.0.1 in PyPI

👍 1

👤 🧑 **serhatci** self-assigned this on Oct 22

Assignees

🧑 **serhatci**

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants