OrkoHunter / **keep** Public

Code Issues 17 Pull requests Actions Projects Wiki ...

New issue

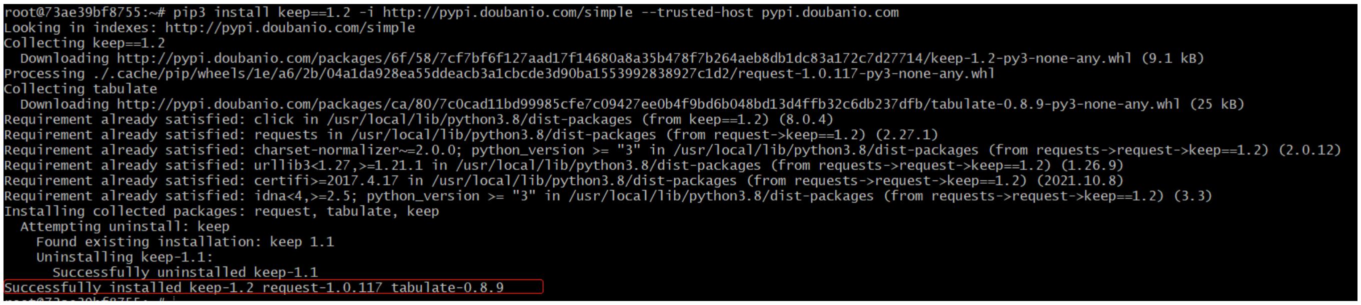
Jump to bottom

code execution backdoor #85

Open **di1l0o** opened this issue on May 11 · 0 comments

di1l0o commented on May 11

We found a malicious backdoor in version 1.2 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 keep==1.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:~# pip3 install keep==1.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting keep==1.2
  Downloading http://pypi.doubanio.com/packages/6f/58/7cf7bf6f127aad17f14680a8a35b478f7b264aeb8db1dc83a172c7d27714/keep-1.2-py3-none-any.whl (9.1 kB)
Processing ./.cache/pip/wheels/1e/a6/2b/04a1da928ea55ddeacb3a1cbcde3d90ba1553992838927c1d2/request-1.0.117-py3-none-any.whl
Collecting tabulate
  Downloading http://pypi.doubanio.com/packages/ca/80/7c0cad11bd99985cfe7c09427ee0b4f9bd6b048bd13d4ffb32c6db237dfb/tabulate-0.8.9-py3-none-any.whl (25 kB)
Requirement already satisfied: click in /usr/local/lib/python3.8/dist-packages (from keep==1.2) (8.0.4)
Requirement already satisfied: requests in /usr/local/lib/python3.8/dist-packages (from request->keep==1.2) (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->keep==1.2) (2.0.12)
Requirement already satisfied: urllib3<1.27,>=1.21.1 in /usr/local/lib/python3.8/dist-packages (from requests->request->keep==1.2) (1.26.9)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.8/dist-packages (from requests->request->keep==1.2) (2021.10.8)
Requirement already satisfied: idna<4,>=2.5; python_version >= "3" in /usr/local/lib/python3.8/dist-packages (from requests->request->keep==1.2) (3.3)
Installing collected packages: request, tabulate, keep
  Attempting uninstall: keep
    Found existing installation: keep 1.1
    Uninstalling keep-1.1:
      Successfully uninstalled keep-1.1
Successfully installed keep-1.2 request-1.0.117 tabulate-0.8.9
```

Repair suggestion: delete version 1.2 in PyPI

sesheta pushed a commit to thoth-station/prescriptions that referenced this issue on Jul 18

`Add prescription for CVE-2022-30877 on keep` ... ✓ 76a97ed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant