esdc-esac-esa-int / **pyesasky** Public

Code Issues 4 Pull requests 15 Actions Projects Security ···

New issue

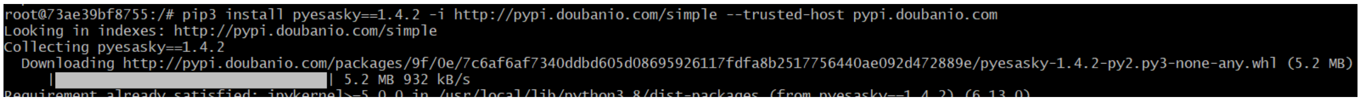
Jump to bottom

code execution backdoor #39

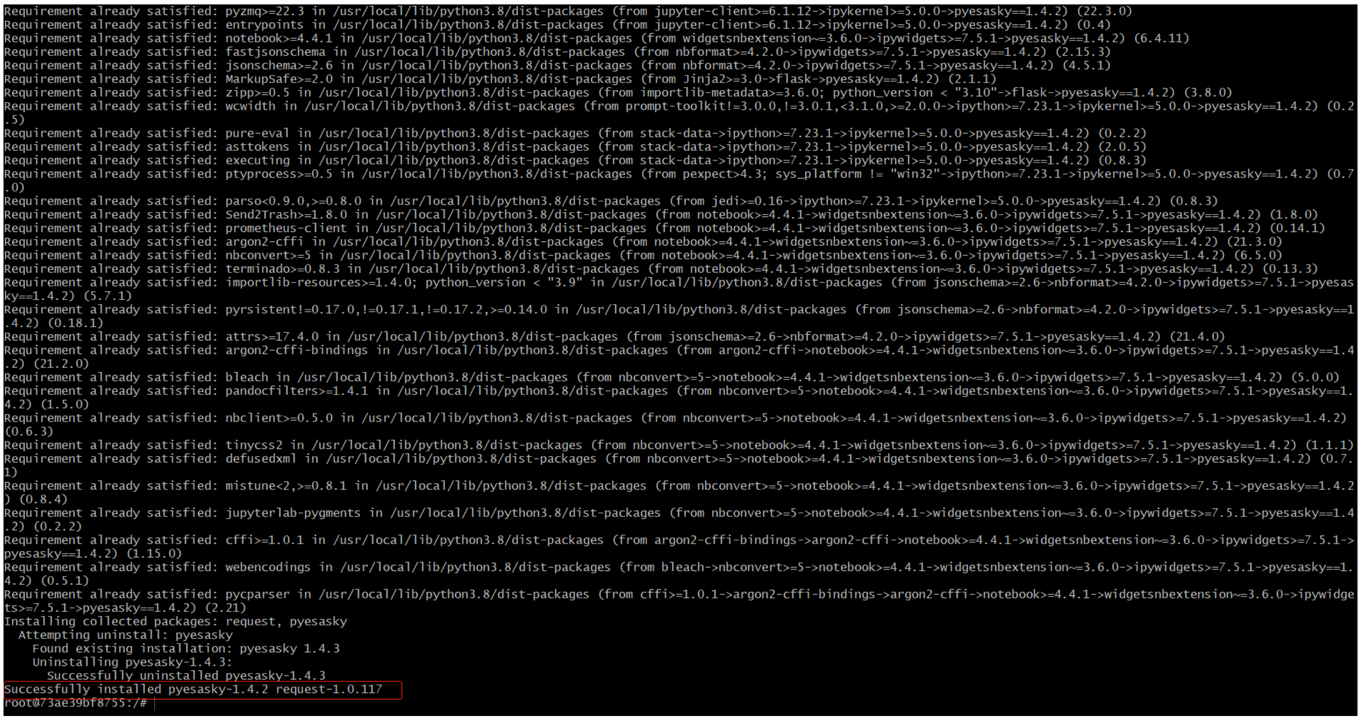
Open **di1l0o** opened this issue on May 14 · 0 comments

di1l0o commented on May 14

We found a malicious backdoor in versions 1.2.0~1.4.2 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 pyesasky==1.4.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com, the request malicious plugin can be successfully installed.



```
root@73ae39bf8755:/# pip3 install pyesasky==1.4.2 -i http://pypi.doubanio.com/simple --trusted-host pypi.doubanio.com
Looking in indexes: http://pypi.doubanio.com/simple
Collecting pyesasky==1.4.2
  Downloading http://pypi.doubanio.com/packages/9f/0e/7c6af6af7340ddbd605d08695926117fdfa8b2517756440ae092d472889e/pyesasky-1.4.2-py2.py3-none-any.whl (5.2 MB)
     |████████████████████████████████| 5.2 MB 932 kB/s
Requirement already satisfied: ipykernel>=5.0.0 in /usr/local/lib/python3.8/dist-packages (from pyesasky==1.4.2) (6.13.0)
```



```
Requirement already satisfied: pyzmq>=22.3 in /usr/local/lib/python3.8/dist-packages (from jupyter-client>=6.1.12->ipykernel>=5.0.0->pyesasky==1.4.2) (22.3.0)
Requirement already satisfied: entrypoints in /usr/local/lib/python3.8/dist-packages (from jupyter-client>=6.1.12->ipykernel>=5.0.0->pyesasky==1.4.2) (0.4)
Requirement already satisfied: notebook>=4.4.1 in /usr/local/lib/python3.8/dist-packages (from widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (6.4.11)
Requirement already satisfied: fastjsonschema in /usr/local/lib/python3.8/dist-packages (from nbformat>=4.2.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (2.15.3)
Requirement already satisfied: jsonschema>=2.6 in /usr/local/lib/python3.8/dist-packages (from nbformat>=4.2.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (4.5.1)
Requirement already satisfied: MarkupSafe>=2.0 in /usr/local/lib/python3.8/dist-packages (from Jinja2>=3.0->flask->pyesasky==1.4.2) (2.1.1)
Requirement already satisfied: zipp>=0.5 in /usr/local/lib/python3.8/dist-packages (from importlib-metadata>=3.6.0; python_version < "3.10"->flask->pyesasky==1.4.2) (3.8.0)
Requirement already satisfied: wcwidth in /usr/local/lib/python3.8/dist-packages (from prompt-toolkit!=3.0.0,!=3.0.1,<3.1.0,>=2.0.0->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (0.2
.5)
Requirement already satisfied: pure-eval in /usr/local/lib/python3.8/dist-packages (from stack-data->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (0.2.2)
Requirement already satisfied: asttokens in /usr/local/lib/python3.8/dist-packages (from stack-data->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (2.0.5)
Requirement already satisfied: executing in /usr/local/lib/python3.8/dist-packages (from stack-data->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (0.8.3)
Requirement already satisfied: ptyprocess>=0.5 in /usr/local/lib/python3.8/dist-packages (from pexpect>4.3; sys_platform != "win32"->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (0.7
.0)
Requirement already satisfied: parso<0.9.0,>=0.8.0 in /usr/local/lib/python3.8/dist-packages (from jedi>=0.16->ipython>=7.23.1->ipykernel>=5.0.0->pyesasky==1.4.2) (0.8.3)
Requirement already satisfied: Send2Trash>=1.8.0 in /usr/local/lib/python3.8/dist-packages (from notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (1.8.0)
Requirement already satisfied: prometheus-client in /usr/local/lib/python3.8/dist-packages (from notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (0.14.1)
Requirement already satisfied: argon2-cffi in /usr/local/lib/python3.8/dist-packages (from notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (21.3.0)
Requirement already satisfied: nbconvert>=5 in /usr/local/lib/python3.8/dist-packages (from notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (6.5.0)
Requirement already satisfied: terminado>=0.8.3 in /usr/local/lib/python3.8/dist-packages (from notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (0.13.3)
Requirement already satisfied: importlib-resources>=1.4.0; python_version < "3.9" in /usr/local/lib/python3.8/dist-packages (from jsonschema>=2.6->nbformat>=4.2.0->ipywidgets>=7.5.1->pyesas
ky==1.4.2) (5.7.1)
Requirement already satisfied: pyrsistent!=0.17.0,!=0.17.1,!=0.17.2,>=0.14.0 in /usr/local/lib/python3.8/dist-packages (from jsonschema>=2.6->nbformat>=4.2.0->ipywidgets>=7.5.1->pyesasky==1
.4.2) (0.18.1)
Requirement already satisfied: attrs>=17.4.0 in /usr/local/lib/python3.8/dist-packages (from jsonschema>=2.6->nbformat>=4.2.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (21.4.0)
Requirement already satisfied: argon2-cffi-bindings in /usr/local/lib/python3.8/dist-packages (from argon2-cffi->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4
.2) (21.2.0)
Requirement already satisfied: bleach in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (5.0.0)
Requirement already satisfied: pandocfilters>=1.4.1 in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.
4.2) (1.5.0)
Requirement already satisfied: nbclient>=0.5.0 in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2)
(0.6.3)
Requirement already satisfied: tinycss2 in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (1.1.1)
Requirement already satisfied: defusedxml in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2) (0.7.
1)
Requirement already satisfied: mistune<2,>=0.8.1 in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4.2
) (0.8.4)
Requirement already satisfied: jupyterlab-pygments in /usr/local/lib/python3.8/dist-packages (from nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.4
.2) (0.2.2)
Requirement already satisfied: cffi>=1.0.1 in /usr/local/lib/python3.8/dist-packages (from argon2-cffi-bindings->argon2-cffi->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->
pyesasky==1.4.2) (1.15.0)
Requirement already satisfied: webencodings in /usr/local/lib/python3.8/dist-packages (from bleach->nbconvert>=5->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidgets>=7.5.1->pyesasky==1.
4.2) (0.5.1)
Requirement already satisfied: pycparser in /usr/local/lib/python3.8/dist-packages (from cffi>=1.0.1->argon2-cffi-bindings->argon2-cffi->notebook>=4.4.1->widgetsnbextension~=3.6.0->ipywidge
ts>=7.5.1->pyesasky==1.4.2) (2.21)
Installing collected packages: request, pyesasky
  Attempting uninstall: pyesasky
    Found existing installation: pyesasky 1.4.3
    Uninstalling pyesasky-1.4.3:
      Successfully uninstalled pyesasky-1.4.3
Successfully installed pyesasky-1.4.2 request-1.0.117
root@73ae39bf8755:/#
```

Repair suggestion: delete version 1.2.0~1.4.2 in PyPI.

Assignees

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant