**Numpy-pad漏洞：**

Numpy是Tensorflow所依赖的一个科学计算的python库，Tensorflow在进行进行矩阵运算多会使用该库。该漏洞发现于librosa库中，librosa.stft函数调用了numpy.pad函数，但是其对于输入的验证并不完整，只验证了声道数等参数，并未对输入array是否为空进行验证，但是其开发者认为这是Numpy的漏洞。

该漏洞是由于numpy.pad（array, pad\_width, mode）函数对于输入的array没有进行验证，当传入的array是一个空数组时，使得safe\_pad参数为-1，该参数正常情况下是一个不断增大的正数，最终当 pad\_before>safe\_pad和pad\_after>safe\_pad同时不成立时，while循环结束。而当其为-1时，使得pad\_iter\_b和pad\_iter\_a也为负数，safe\_pad不断加负数，使得循环始终无法结束，从而导致拒绝服务，具体代码如图1所示。

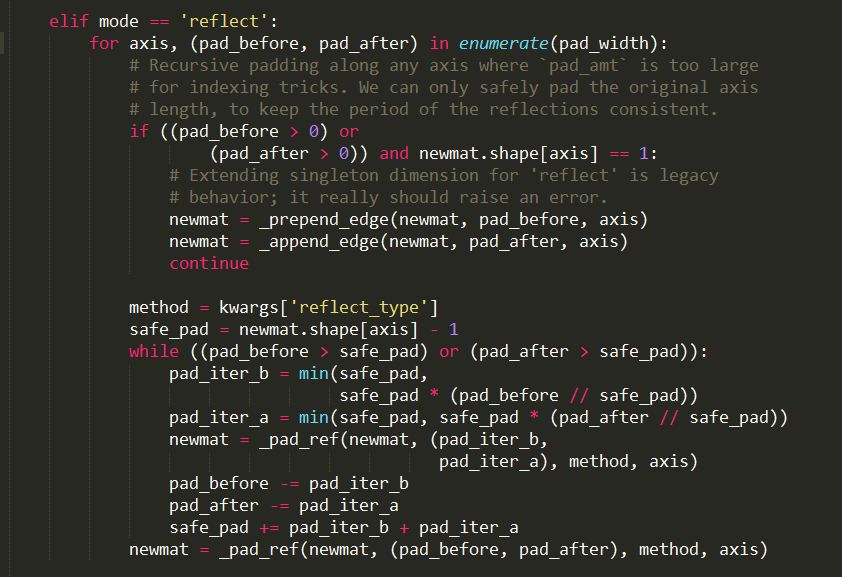


图1 Numpy-pad漏洞代码

该漏洞的代码位于Numpy/numpy/lib/arraypad.py文件中。

该漏洞影响librosa-0.5.1及以下版本，Numpy-1.13.1及以下版本，以及其他使用Numpy.pad（xx, xx, mode=’reflect’）函数的功能模块；在Numpy-1.13.2已修复。

触发该漏洞的代码：

|  |
| --- |
| **import numpy as np**  **np.pad([],10,’reflect’) 或 np.pad(np.ndarray(0),10,’reflect’)** |

无限循环效果：

|  |
| --- |
| iter\_b: -1  iter\_a: -1  before: 101  after: 101  safe\_pad: -3  safe\_0: -1  iter\_b: -3  iter\_a: -3  before: 104  after: 104  safe\_pad: -9  safe\_0: -1  iter\_b: -9  iter\_a: -9  before: 113  after: 113  safe\_pad: -27  safe\_0: -1  iter\_b: -27  iter\_a: -27  before: 140  after: 140  safe\_pad: -81  safe\_0: -1  iter\_b: -81  iter\_a: -81  before: 221  after: 221  safe\_pad: -243  safe\_0: -1 |