VigiZhang add pdsa-2022-002 (#47486) History

1 contributor

33 lines (23 sloc) | 1.02 KB ...

PDSA-2022-002: Code injection in paddle.audio.functional.get_window

Impact

`paddle.audio.functional.get_windowis` vulnerable to a code injection as it calls `eval` on user supplied `winstr`. This may lead to arbitrary code execution.

```
def get_window(
    window: Union[str, Tuple[str, float]],
    win_length: int,
    fftbins: bool = True,
    dtype: str = 'float64',
) -> Tensor:
    ...
    try:
        winfunc = eval('_' + winstr)
    except NameError as e:
        raise ValueError("Unknown window type.") from e
```

Patches

We have patched the issue in commit 26c419ca386aeae3c461faf2b828d00b48e908eb.

The fix will be included in PaddlePaddle 2.4.

For more information

Please consult our security guide for more information regarding the security model and how to contact us with issues and questions.

Attribution

This vulnerability has been reported by Tong Liu of ShanghaiTech University.