

Components:

apache pyarrow *

Description:

Deserialization of untrusted data in IPC and Parquet readers in PyArrow versions 0.14.0 to 14.0.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example user-supplied input files). This vulnerability only affects PyArrow, not other Apache Arrow implementations or bindings. It is recommended that users of PyArrow upgrade to 14.0.1. Similarly, it is recommended that downstream libraries upgrade their dependency requirements to PyArrow 14.0.1 or later. PyPI packages are already available, and we hope that conda-forge packages will be available soon. If it is not possible to upgrade, we provide a separate package 'pyarrow-hotfix' that disables the vulnerability on older PyArrow versions. See <https://pypi.org/project/pyarrow-hotfix/> for instructions.

Main problems:

502 "Deserialization of Untrusted Data"