

apache superset *

Description:

If an attacker gains write access to the Apache Superset metadata database, they could persist a specifically crafted Python object that may lead to remote code execution on Superset's web backend. The Superset metadata db is an 'internal' component that is typically only accessible directly by the system administrator and the superset process itself. Gaining access to that database should be difficult and require significant privileges. This vulnerability impacts Apache Superset versions 1.5.0 up to and including 2.1.0. Users are recommended to upgrade to version 2.1.1 or later.

Main problems:

502 "Deserialization of Untrusted Data"