huntr

Insecure Temporary File in mlflow/mlflow

0

✓ Valid Reported on Jan 8th 2022

Description

`mlflow` package is using the deprecated function `tempfile.mktemp()` which is not secure. Because a different process may create a file with this name in the time between the call to `mktemp()` and the subsequent attempt to create the file by the first process.

Impact

Availability will get affected because of this vulnerability.

Remediation

Use `mkstemp()` instead of `tempfile.mktemp()`

Occurrences

file_utils.py L290

References

- https://docs.python.org/3/library/tempfile.html#deprecated-functions-and-variables

CVE
CVE-2022-0736
(Published)

Vulnerability Type
CWE-377: Insecure Temporary File

Severity
High (8.2)

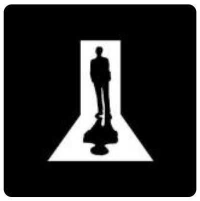
Chat with us

Visibility

Visibility
Public

Status
Fixed

Found by



Srikanth Prathi
@srikanthprathi
unranked

This report was seen 462 times.

We are processing your report and will contact the **mlflow** team within 24 hours. a year ago

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

Corey Zumar validated this vulnerability 9 months ago

Srikanth Prathi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Corey Zumar marked this as fixed in **1.23.1** with commit **61984e** 9 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

file_utils.py#L290 has been validated ✓

Sign in to join this conversation

2022 © 418sec

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us