Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of an Absolute Path Traversal vulnerability in GitHub repository mlflow/mlflow prior to 2.5.0.

Technical Details

The *validate_path_is_safe()* function in file /mlflow/server/handlers.py, introduced in PR #7891 on Feb 24th, 2023 does not account for Windows absolute path format, and thus can be bypassed on MLFlow servers, running on Windows hosts, exposing them to a number of high-impact directory traversals.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-3765
- https://github.com/mlflow/mlflow/commit/6dde93758d42455cb90ef324407919ed67668b9b
- https://huntr.dev/bounties/4be5fd63-8a0a-490d-9ee1-f33dc768ed76