# CVE Detail – CVE-2024-4315

parisneo/lollms version 9.5 is vulnerable to Local File Inclusion (LFI) attacks due to insufficient path sanitization. The `sanitize\_path\_from\_endpoint` function fails to properly sanitize Windows-style paths (backward slash `\`), allowing attackers to perform directory traversal attacks on Windows systems. This vulnerability can be exploited through various routes, including `personalities` and `/del\_preset`, to read or delete any file on the Windows filesystem, compromising the system's availability.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.68434

## CVSS Scoring

CVSS v3.0 Score: 9.1

Severity: CRITICAL

## Mapped CWE(s)

* CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')

## CAPEC(s)

* CAPEC-193: PHP Remote File Inclusion