UNC SSRF/NTLMv2 Credential Theft/Local File Read in static resource handler on Windows

Low **Dreamsorcerer** published **GHSA-p998-jp59-783m** 20 hours ago

Package

aiohttp (pip)

Affected versions

<=3.13.3

Patched versions

3.13.4

Description

Summary

On Windows the static resource handler may expose information about a NTLMv2 remote path.

Impact

If an application is running on Windows, and using aiohttp's static resource handler (not recommended in production), then it may be possible for an attacker to extract the hash from an NTLMv2 path and then extract the user's credentials from there.

Patch: `0ae2aa0`

Severity

Low

CVE ID

CVE-2026-34515

Weaknesses

- CWE-36
- CWE-918

Credits

nvn1729	Reporter
bdraco	Remediation developer