## Results for Vulnerability Scan

I decided to run a vulnerability scan on an observability project using Python since it contained some third-party packages. The purpose of the project was for observability testing. The scan showed two packages with three vulnerabilities in the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Vulnerability | Version/Severity | Fix Version |
| **Requests**  (GHSA-9hjg-9r4m-mvj7) | URL parsing flaw may leak .netrc credentials via malicious URLs | 2.32.3/High | 2.32.4 |
| urllib3 (GHSA-48p4-8xcf-vxj5) | Redirect control ignored in Pyodide/JS runtimes (possible SSRF bypass) | 2.3.0/Medium | 2.5.0 |
| GHSA-pq67-6m6q-mj2v) | retries ignored at PoolManager level (redirects still followed) | 2.3.0/Medium | 2.5.0 |

## Detailed Findings and Mitigations

**1. Requests (2.32.3) – High Severity**  
– *Description:* URL parsing flaw may leak .netrc credentials.  
– *Mitigation:* Upgrade to requests ≥ 2.32.4 with uv add requests@latest. If upgrading isn’t possible immediately, set trust\_env=False to disable .netrc.

**2. Urllib3 (GHSA-48p4-8xcf-vxj5) – Medium Severity**  
– *Description:* Redirect control ignored in Pyodide/JS runtimes.  
– *Mitigation:* Upgrade to urllib3 ≥ 2.5.0 with uv add urllib3@latest. Also add SSRF protections at the application layer.

**3. Urllib3 (GHSA-pq67-6m6q-mj2v) – Medium Severity**  
– *Description:* retries ignored at PoolManager level so redirects cannot be globally disabled.  
– *Mitigation:* Upgrade to urllib3 ≥ 2.5.0 with uv add urllib3@latest. In the meantime, disable redirects at each request() call instead of globally.