CHANGES AI

Vulnerability Remediation Report

AI-assisted change-impact analysis for Python software dependencies.

REPORT DETAILS

RUN ID	67
TARGET	`/path/to/target`
PACKAGES ANALYSED	15
VULNERABILITIES FOUND	17
REMEDIATION PATHS	3
GENERATED	27 April 2026 · 04:53 UTC

Executive Summary

The project shows a concentrated but manageable vulnerability surface: 4 HIGH, 10 MEDIUM and 3 LOW findings across 15 packages, dominated by multiple HIGH issues in urllib3 and a HIGH in black. Three remediation pathways were modeled. The maximum-coverage path eliminates the most fixes (16 CVEs) but accepts higher-risk upgrades (notably pytest and virtualenv) and carries the largest breakage score, so it demands substantial testing and compatibility work. The balanced path resolves nearly as many issues (15 CVEs) while avoiding the single highest-breakage pytest upgrade, reducing regression risk at the cost of leaving one open CVE and one vendor-no-fix pip issue that must be mitigated operationally. The minimum-breakage path makes only the smallest set of changes (upgrading the packages that remove immediate HIGH exposure) and minimizes churn but leaves most CVEs unaddressed and yields higher residual exposure.

Likely upgrade risk is medium: several candidate upgrades (pytest, virtualenv) have the highest breakage potential and impact testing/tooling, while upgrades for black, pip, and urllib3 are lower-risk. Confidence in impact estimates is medium and there is an unresolved dynamic import for PyYAML that could affect analysis.

The most important remediation outcome is to remove the immediate HIGH exposure by upgrading urllib3 to the fixed 2.6.x line and black to the fixed 26.3.1, then adopt the balanced upgrade wave for the remainder—deferring the risky pytest bump until after focused testing. For the pip CVE with no vendor fix, apply operational mitigations (restrict/pin pip in production images and monitor for vendor fixes).

Vulnerabilities by Severity

- HIGH: 4
- MEDIUM: 10
- LOW: 3

SEVERITY	PACKAGE	INSTALLED	ID	FIXED IN
HIGH	black	25.9.0	GHSA-3936-cmfr-pm3m	26.3.1
HIGH	urllib3	2.5.0	GHSA-2xpw-w6gg-jr37	2.6.0
HIGH	urllib3	2.5.0	GHSA-38jv-5279-wg99	2.6.3
HIGH	urllib3	2.5.0	GHSA-gm62-xv2j-4w53	2.6.0
MEDIUM	Werkzeug	3.1.3	GHSA-29vq-49wr-vm6x	3.1.6
MEDIUM	Werkzeug	3.1.3	GHSA-87hc-h4r5-73f7	3.1.5
MEDIUM	Werkzeug	3.1.3	GHSA-hgf8-39gv-g3f2	3.1.4
MEDIUM	filelock	3.20.0	GHSA-qmgc-5h2g-mvrw	3.20.3
MEDIUM	filelock	3.20.0	GHSA-w853-jp5j-5j7f	3.20.1
MEDIUM	pip	25.3	GHSA-58qw-9mgm-455v	none known
MEDIUM	pytest	8.4.2	GHSA-6w46-j5rx-g56g	9.0.3
MEDIUM	python-dotenv	1.2.1	GHSA-mf9w-mj56-hr94	1.2.2
MEDIUM	requests	2.32.5	GHSA-gc5v-m9x4-r6x2	2.33.0
MEDIUM	virtualenv	20.35.4	GHSA-597g-3phw-6986	20.36.1
LOW	Pygments	2.19.2	GHSA-5239-wwwm-4pmq	2.20.0
LOW	flask	3.1.2	GHSA-68rp-wp8r-4726	3.1.3
LOW	pip	25.3	GHSA-6vgw-5pg2-w6jp	26.0

Currency Signals

PACKAGE	INSTALLED	LATEST	LATEST RELEASE	CADENCE (DAYS)	SIGNALS
PyYAML	6.0.3	6.0.3	2025-09-25T21:31:46Z	360.8	slow_release_cadence
bandit	1.8.6	1.9.4	2026-02-25T06:44:13Z	58.5	none
breathe	4.36.0	4.36.0	2025-02-22T18:36:01Z	278.5	slow_release_cadence
flask	3.1.2	3.1.3	2026-02-19T05:00:56Z	170.6	none
flask-cors	6.0.1	6.0.2	2025-12-12T20:31:41Z	72.9	none
flask-socketio	5.5.1	5.6.1	2026-02-21T13:07:51Z	127.0	none
myst-parser	4.0.1	5.0.0	2026-01-15T09:08:16Z	157.9	major_version_lag:1
openai	2.6.1	2.32.0	2026-04-15T22:28:17Z	8.3	none
pyoslog	1.2.0	1.2.0	2025-05-28T08:32:44Z	247.2	slow_release_cadence
python-dotenv	1.2.1	1.2.2	2026-03-01T16:00:25Z	85.3	none
python-socketio	5.14.3	5.16.1	2026-02-06T23:42:05Z	25.1	none
sphinx	8.2.3	9.1.0	2025-12-31T15:09:25Z	6.9	major_version_lag:1
sphinx-autodoc-typehints	3.5.2	3.10.2	2026-04-15T22:09:47Z	5.7	none
sphinx-rtd-theme	3.0.2	3.1.0	2026-01-12T16:03:28Z	115.0	none
sphinxcontrib-mermaid	1.0.0	2.0.1	2026-03-05T14:10:40Z	24.9	major_version_lag:1

Used-Symbol Summary

- PyYAML: yaml
- flask: Flask, jsonify, render_template, request, send_from_directory
- flask-cors: CORS
- flask-socketio: SocketIO, emit
- openai: AsyncOpenAI, Response, ResponseInputItemParam, ToolParam
- pyoslog: pyoslog
- pytest: pytest
- python-dotenv: load_dotenv

Unresolved usage flags: - dynamic_import (PyYAML): run_agent.py:64

Impact Summary

PACKAGE	UPGRADE	BREAKAGE	CONFIDENCE
Pygments	2.19.2 -> 2.20.0	LOW (0.12)	MEDIUM
Werkzeug	3.1.3 -> 3.1.4	LOW (0.05)	MEDIUM
Werkzeug	3.1.3 -> 3.1.8	LOW (0.12)	MEDIUM
black	25.9.0 -> 26.3.1	LOW (0.15)	MEDIUM
filelock	3.20.0 -> 3.20.1	LOW (0.05)	MEDIUM
filelock	3.20.0 -> 3.29.0	LOW (0.12)	MEDIUM
flask	3.1.2 -> 3.1.3	NONE (0.02)	HIGH
pip	25.3 -> 26.0	LOW (0.15)	MEDIUM
pip	25.3 -> 26.1	LOW (0.15)	MEDIUM
pytest	8.4.2 -> 9.0.3	MEDIUM (0.45)	MEDIUM
python-dotenv	1.2.1 -> 1.2.2	LOW (0.12)	MEDIUM
requests	2.32.5 -> 2.33.0	LOW (0.12)	MEDIUM
requests	2.32.5 -> 2.33.1	LOW (0.12)	MEDIUM
urllib3	2.5.0 -> 2.6.0	LOW (0.12)	MEDIUM
urllib3	2.5.0 -> 2.6.3	LOW (0.12)	MEDIUM
virtualenv	20.35.4 -> 20.36.1	LOW (0.15)	MEDIUM
virtualenv	20.35.4 -> 21.2.4	MEDIUM (0.45)	MEDIUM

> Pygments 2.19.2 -> 2.20.0: Release indicates 2.20.0 fixes GHSA-5239 (low severity). Changelog and release notes do not document breaking API removals, and the provided project usage list contains no Pygments symbols, so direct impact on the project is unlikely. Citation: metadata_changelog - Changelog (https://github.com/pygments/pygments/blob/master/CHANGES)

Werkzeug 3.1.3 -> 3.1.4: Version 3.1.4 is a patch release that fixes GHSA-hgf8-39gv-g3f2 for versions < 3.1.4. It is unlikely to introduce breaking API changes, but other listed vulnerabilities remain fixed only in later versions (3.1.5 and 3.1.6) and are not addressed by this upgrade. Citation: metadata_changelog - Changes (https://werkzeug.palletsprojects.com/page/changes/)

Werkzeug 3.1.3 -> 3.1.8: CVE records show fixes introduced in 3.1.4–3.1.6 and the candidate (3.1.8) is patch-level; release notes and CVE descriptions indicate security hardenings to URL and header handling rather than public API removals, so breaking risk is low but behavioral changes may affect edge-case inputs. Citation: metadata_changelog - Changes (https://werkzeug.palletsprojects.com/page/changes/)

black 25.9.0 -> 26.3.1: The GHSA-3936-cmfr-pm3m vulnerability is fixed in 26.3.1; the project shows no detected imports/usages of black so upgrading primarily affects developer tooling/CI rather than runtime application code. Major-version upgrades can include CLI, configuration, or API signature changes, so validate CI and any programmatic calls to black after updating. Citation: metadata_changelog - Changelog (https://github.com/psf/black/blob/main/CHANGES.md)

filelock 3.20.0 -> 3.20.1: 3.20.1 is a patch release that addresses GHSA-w853-jp5j-5j7f (medium); the other reported issue (GHSA-qmgc-5h2g-mvrw) is fixed in 3.20.3 and remains unaddressed by 3.20.1. With no release notes or observed API usage, the upgrade is likely low-risk but not fully verifiable.

filelock 3.20.0 -> 3.29.0: The CVE records show fixes introduced in 3.20.1 and 3.20.3, indicating these were security patches within the 3.20 series; moving to 3.29.0 is a minor-version upgrade and is unlikely to remove or widely change existing public APIs, and no project symbols were reported as used.

flask 3.1.2 -> 3.1.3: GHSA-68rp-wp8r-4726 (LOW) is fixed in 3.1.3. The release is a patch-level update with no documented API removals or signature changes affecting common symbols (Flask, jsonify, render_template, send_from_directory, request), so upgrading should be safe. Citation: metadata_changelog - Changes (https://flask.palletsprojects.com/page/changes/)

pip 25.3 -> 26.0: pip is primarily a command-line installer rather than a stable importable library; the upgrade from 25.3 to 26.0 is a major bump and the changelog notes changes in 26.x, and one CVE (GHSA-6vgw-5pg2-w6jp) is fixed in 26.0 while another GHSA record has no fixed version listed, indicating security motivation for the upgrade. Citation: metadata_changelog - Changelog (https://pip.pypa.io/en/stable/news/)

pip 25.3 -> 26.1: pip is primarily used as an external installer (CLI) so most application code will not break; the security advisory GHSA-6vgw-5pg2-w6jp lists fixes beginning at 26.0 (26.1 includes them).

Internal pip APIs (pip._internal) are known to change between major releases and could break code that imports them. Citation: metadata_changelog - Changelog (https://pip.pypa.io/en/stable/news/)

pytest 8.4.2 -> 9.0.3: This is a major-version upgrade; the changelog and release notes for 9.0.3 indicate breaking changes and removals in plugin and config internals. The security advisory (GHSA-6w46-j5rx-g56g) is fixed in 9.0.3, so upgrading removes the reported vulnerability. Citation: metadata_changelog - Changelog (https://docs.pytest.org/en/stable/changelog.html)

python-dotenv 1.2.1 -> 1.2.2: CVE GHSA-mf9w-mj56-hr94 is fixed in 1.2.2 (affects <1.2.2), indicating a security fix. Because this is a patch bump, API signatures are unlikely to change, but parsing/validation behaviour that affects load_dotenv may be hardened, creating low risk of minor behavioral differences.

requests 2.32.5 -> 2.33.0: The candidate 2.33.0 is a minor bump that fixes GHSA-gc5v-m9x4-r6x2; there is no available release evidence of API removals or signature changes, and Requests typically avoids breaking changes in minor releases.

requests 2.32.5 -> 2.33.1: GHSA-gc5v-m9x4-r6x2 is fixed in 2.33.0, so upgrading to 2.33.1 resolves that vulnerability. No project usage symbols were supplied and no changelog evidence was provided, so the assessment assumes a low-risk minor release focused on security/bug fixes.

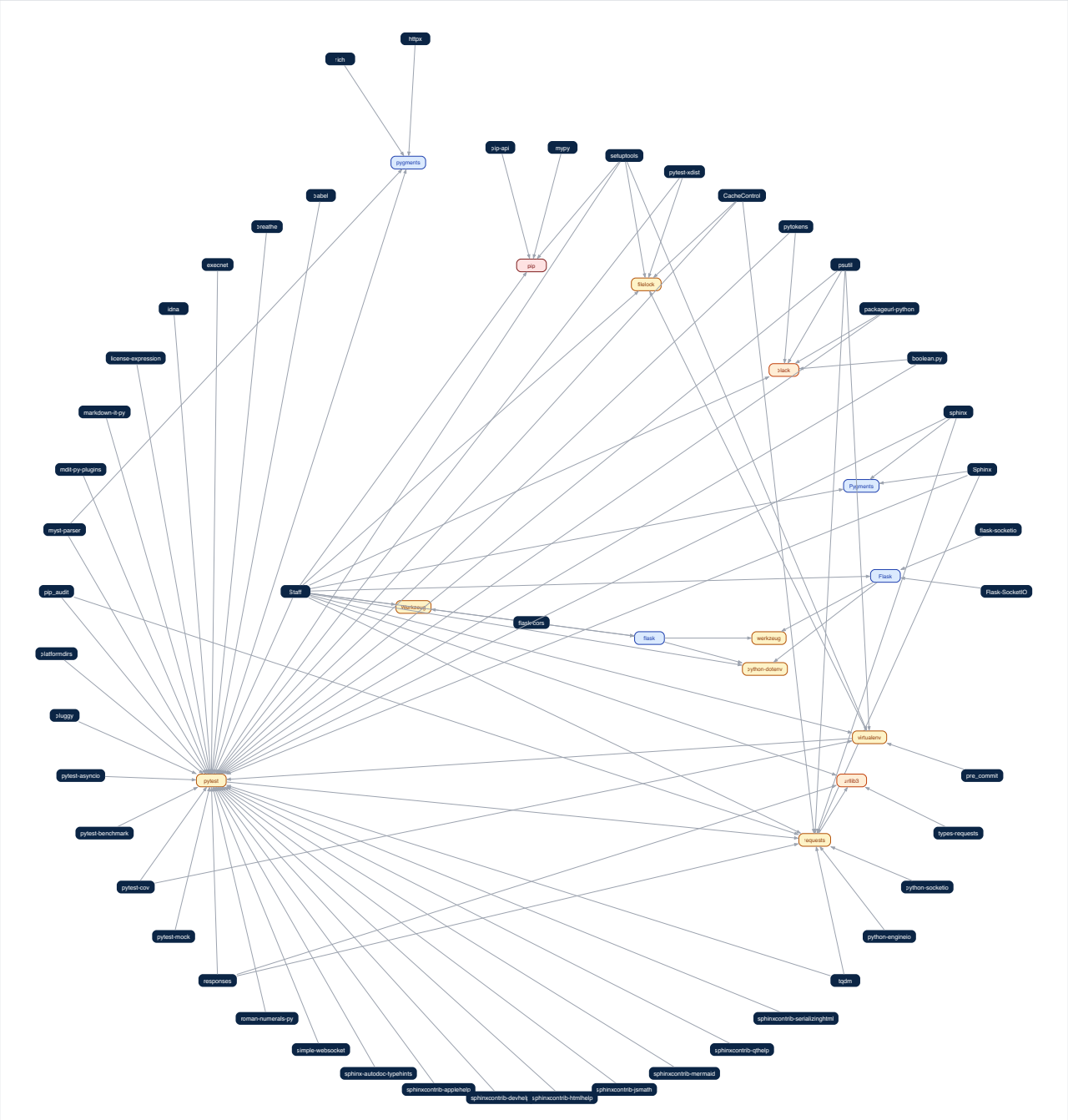
urllib3 2.5.0 -> 2.6.0: Upgrading from 2.5.0 to 2.6.0 patches GHSA-2xpw-w6gg-jr37 and GHSA-gm62-xv2j-4w53 but does not fix GHSA-38jv-5279-wg99 (which is fixed in 2.6.3). The bump is a minor release, so breaking API changes are unlikely for typical usage, and the project provided no symbol usage indicating direct exposure. Citation: metadata_changelog - Changelog (https://github.com/urllib3/urllib3/blob/main/CHANGES.rst)

urllib3 2.5.0 -> 2.6.3: Upgrade from 2.5.0 to 2.6.3 includes fixes for multiple HIGH-severity advisories (fixed in 2.6.0 and 2.6.3). This is a minor-version bump within 2.x, so breaking API changes are unlikely, but project-specific usage wasn't supplied so residual risk remains. Citation: metadata_changelog - Changelog (https://github.com/urllib3/urllib3/blob/main/CHANGES.rst)

virtualenv 20.35.4 -> 20.36.1: The CVE GHSA-597g-3phw-6986 is fixed in 20.36.1 and the upgrade is a minor bump within the 20.x series, implying limited API change risk. The project reports no used symbols from virtualenv, so direct breakage risk to this codebase is unlikely.

virtualenv 20.35.4 -> 21.2.4: The upgrade is a major-version jump (20.35.4 -> 21.2.4) and the security fix referenced applies to <20.36.1, so the candidate includes the fix. Major releases of virtualenv frequently reorganize APIs and seeding behaviour, so there is a moderate risk of breakage for projects that call virtualenv programmatically.

Dependency Graph



KEY: High Medium Low No fix available

Ranked Remediation Paths

BALANCED

EXPOSURE **0.076** BREAKAGE **0.15** CONFIDENCE **MEDIUM**

This path prioritizes fixing all HIGH-severity issues and the majority of MEDIUMs while avoiding the highest breakage upgrade (pytest 9.0.3). It uses candidate versions from the impact reports that have low-to-moderate breakage scores to keep regression risk manageable. One medium-severity pytest CVE is deferred to reduce churn during the upgrade wave; operational hardening should be used for the pip no-fix CVE. Confidence is medium because most impact reports are complete but several items have unresolved usage flags.

PACKAGE	FROM	TO	FIXES
python-dotenv	1.2.1	1.2.2	GHSA-mf9w-mj56-hr94
flask	3.1.2	3.1.3	GHSA-68rp-wp8r-4726
requests	2.32.5	2.33.0	GHSA-gc5v-m9x4-r6x2
urllib3	2.5.0	2.6.3	GHSA-2xpw-w6gg-jr37, GHSA-38jv-5279-wg99, GHSA-gm62-xv2j-4w53
pip	25.3	26.0	GHSA-6vgw-5pg2-w6jp
black	25.9.0	26.3.1	GHSA-3936-cmfr-pm3m
Werkzeug	3.1.3	3.1.8	GHSA-29vq-49wr-vm6x, GHSA-87hc-h4r5-73f7, GHSA-hgf8-39gv-g3f2
Pygments	2.19.2	2.20.0	GHSA-5239-wwwm-4pmq
filelock	3.20.0	3.29.0	GHSA-qmgc-5h2g-mvrw, GHSA-w853-jp5j-5j7f
virtualenv	20.35.4	20.36.1	GHSA-597g-3phw-6986

NO FIX AVAILABLE GHSA-58qw-9mgm-455v Open: GHSA-6w46-j5rx-g56g

MAXIMUM COVERAGE

EXPOSURE **0.038** BREAKAGE **0.45** CONFIDENCE **MEDIUM**

This path applies all candidate upgrades available in the impact reports that map to fixes, eliminating every fixable CVE in the project. It accepts higher-risk upgrades (notably pytest) to maximize coverage; impact reports show pytest as the largest single breakage contributor. The trade-off is more testing and possible compatibility work during rollout. The pip CVE with no vendor fix is left as a no-fix and should be mitigated by operational controls.

PACKAGE	FROM	TO	FIXES
python-dotenv	1.2.1	1.2.2	GHSA-mf9w-mj56-hr94
flask	3.1.2	3.1.3	GHSA-68rp-wp8r-4726
requests	2.32.5	2.33.0	GHSA-gc5v-m9x4-r6x2
urllib3	2.5.0	2.6.3	GHSA-2xpw-w6gg-jr37, GHSA-38jv-5279-wg99, GHSA-gm62-xv2j-4w53
pip	25.3	26.0	GHSA-6vgw-5pg2-w6jp
black	25.9.0	26.3.1	GHSA-3936-cmfr-pm3m
Werkzeug	3.1.3	3.1.8	GHSA-29vq-49wr-vm6x, GHSA-87hc-h4r5-73f7, GHSA-hgf8-39gv-g3f2
pytest	8.4.2	9.0.3	GHSA-6w46-j5rx-g56g
Pygments	2.19.2	2.20.0	GHSA-5239-wwwm-4pmq
filelock	3.20.0	3.29.0	GHSA-qmgc-5h2g-mvrw, GHSA-w853-jp5j-5j7f
virtualenv	20.35.4	20.36.1	GHSA-597g-3phw-6986

NO FIX AVAILABLE GHSA-58qw-9mgm-455v

MINIMUM BREAKAGE

EXPOSURE **0.392** BREAKAGE **0.15** CONFIDENCE **MEDIUM**

This path upgrades only the packages that address the highest-severity findings (all urllib3 HIGH CVEs and the BLACK HIGH CVE), minimizing the number of changes while removing immediate critical exposure. Both upgrades are present in the impact reports with low-to-moderate breakage estimates. Remaining CVEs (including a pip CVE with no fix) are left for a later maintenance window to avoid broader churn. Recommended mitigations for the no-fix pip CVE: restrict pip usage in production images, pin pip where needed, and monitor for vendor fixes.

PACKAGE	FROM	TO	FIXES
urllib3	2.5.0	2.6.3	GHSA-2xpw-w6gg-jr37, GHSA-38jv-5279-wg99, GHSA-gm62-xv2j-4w53
black	25.9.0	26.3.1	GHSA-3936-cmfr-pm3m

NO FIX AVAILABLE GHSA-58qw-9mgm-455v Open: GHSA-29vq-49wr-vm6x, GHSA-5239-wwwm-4pmq, GHSA-597g-3phw-6986, GHSA-68rp-wp8r-4726, GHSA-6vgw-5pg2-w6jp, GHSA-6w46-j5rx-g56g, GHSA-87hc-h4r5-73f7, GHSA-gc5v-m9x4-r6x2, GHSA-hgf8-39gv-g3f2, GHSA-mf9w-mj56-hr94, GHSA-qmgc-5h2g-mvrw, GHSA-w853-jp5j-5j7f

LIMITATIONS AND CONFIDENCE NOTES

- Cached reports reflect the data available when the run was recorded.
- Missing usage, unresolved usage, missing changelog evidence, and LLM fallback paths lower confidence.
- LLM-generated results are not guaranteed to be factually accurate and should be verified before being used as a basis for action.