

nextcloud-mcp-server

github.com/cbcoutinho/nextcloud-mcp-server

Scanned 29 October 2026 at 09:48 · Report generated 29 October 2026 · Python · 394 stars

OVERALL ASSESSMENT

High

Combined score 83 · 134 findings after filtering

Summary

43 findings likely need attention, 79 look like noise. Most notable: Detects dynamic code loading: downloading and importing/executing code at runtime [thre... (98% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Medium (50)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Medium (33)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
bandit	Insecure coding patterns in Python source	0	20	54	74
dep_checker	Vulnerable, unpinned or typosquatted dependencies	1	6	42	49
yara	Signatures of malicious behaviour in source files	5	0	4	9
guarddog	Malicious package and install-time behaviour	1	1	0	2

43 of 134 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	guarddog	Detects dynamic code loading: downloading and importing/executing code at runtime [threat-runtime-dynamic-loader]	1	/nextcloud_mcp_server/app.py:883
HIGH	dep_checker	Typosquatting: 'psycopg' is suspiciously similar to 'psycopg2'	1	pyproject.toml
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	5	/.github/workflows/docker-build-publish.yml
MEDIUM	guarddog	Detects access to sensitive files (credentials, configs, keys) [threat-filesystem-read]	1	/nextcloud_mcp_server/alembic/env.py:20
MEDIUM	dep_checker	Unpinned dependency: 'starlette' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	dep_checker	Unpinned dependency: 'httpx' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	dep_checker	Unpinned dependency: 'icalendar' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	dep_checker	Unpinned dependency: 'mcp' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	dep_checker	Unpinned dependency: 'nextcloud-mcp-server' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	dep_checker	Unpinned dependency: 'pillow' has no version lock — supply chain risk	1	pyproject.toml
MEDIUM	bandit	Using xml.etree.ElementTree.fromstring to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree.fromstring with its defusedxml equivalent function or make sure defusedxml.defuse_stdlib() is called	17	/nextcloud_mcp_server/client/dav_errors.py:114

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	bandit	Use of weak MD5 hash for security. Consider usedforsecurity=False	1	/ nextcloud_m cp_server/ providers/ simple.py:64
MEDIUM	bandit	Possible SQL injection vector through string-based query construction.	2	/ nextcloud_m cp_server/ auth/ storage.py:1 656
LOW	bandit	Using escape to parse untrusted XML data is known to be vulnerable to XML attacks. Replace escape with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.	1	/ nextcloud_m cp_server/ client/ webdav.py:10
LOW	bandit	Possible hardcoded password: 'refresh_token'	2	/ nextcloud_m cp_server/ auth/ token_broker .py:677
LOW	bandit	Possible hardcoded password: '[\$_.-]+'	1	/ nextcloud_m cp_server/ redaction.py :153
LOW	bandit	Possible hardcoded password: 'jwt'	1	/ nextcloud_m cp_server/ app.py:983
LOW	bandit	Possible hardcoded password: 'unknown'	1	/ nextcloud_m cp_server/ observabili ty/ metrics.py:1 500
LOW	bandit	Possible hardcoded password: 'none'	1	/ nextcloud_m cp_server/ auth/ oauth_routes .py:1739

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	bandit	Possible hardcoded password: 'NEXTCLOUD_OIDC_CLIENT_SECRET'	1	/nextcloud_mcp_server/config.py:2156
LOW	bandit	Possible hardcoded password: 'client_secret_post'	1	/nextcloud_mcp_server/auth/client_registration.py:122
LOW	bandit	Possible hardcoded password: 'nextcloud'	1	/nextcloud_mcp_server/auth/oauth_routes.py:985
LOW	bandit	Possible hardcoded password: 'NEXTCLOUD_OIDC_TOKEN_TYPE'	1	/nextcloud_mcp_server/config.py:2157
LOW	bandit	Possible hardcoded password: 'Bearer'	2	/nextcloud_mcp_server/app.py:984
LOW	bandit	Using xml.etree.ElementTree to parse untrusted XML data is known to be vulnerable to XML attacks. Replace xml.etree.ElementTree with the equivalent defusedxml package, or make sure defusedxml.defuse_stdlib() is called.	4	/nextcloud_mcp_server/client/webdav.py:5
LOW	bandit	Possible hardcoded password: 'None'	9	/nextcloud_mcp_server/config.py:44
LOW	bandit	Try, Except, Continue detected.	1	/nextcloud_mcp_server/document_processors/_isolation.py:107

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	bandit	Consider possible security implications associated with the subprocess module.	2	/scripts/sqlitequery.py:16
LOW	dep_checker	Loose version constraint: 'python-json-logger>=3.2.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'opentelemetry-instrumentation-logging>=0.49b2' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'opentelemetry-api>=1.28.2' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'python-docx>=1.2.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'python-pptx>=1.0.2' — attacker could push malicious update	1	pyproject.toml
LOW	bandit	subprocess call - check for execution of untrusted input.	2	/scripts/sqlitequery.py:97
LOW	dep_checker	Loose version constraint: 'pyjwt>=2.8.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'pydantic>=2.11.4' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'psycopg>=3.2' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'prometheus-client>=0.21.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'procrastinate>=3.8' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'pypdfium2>=5.9.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'pyroscope-io>=0.8.0' — attacker could push malicious update	1	pyproject.toml

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'pythonvcard4>=0.2.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'qdrant-client>=1.17.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'recurring-ical-events>=3.8.0,<4.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'sqlalchemy>=2.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'uvicorn>=0.30' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'numpy>=1.26' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'opentelemetry-sdk>=1.28.2' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'aiosqlite>=0.20.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'alembic>=1.14.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'anyio>=4.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'authlib>=1.6.5' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'boto3>=1.35.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'botocore>=1.35.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'caldav>=3.0.1,<4.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'click>=8.1.8' — attacker could push malicious update	1	pyproject.toml

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	dep_checker	Loose version constraint: 'cryptography>=42.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'dynaconf>=3.2.13,<4.0' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'fastembed>=0.7.3' — attacker could push malicious update	1	pyproject.toml
LOW	dep_checker	Loose version constraint: 'jinja2>=3.1.6' — attacker could push malicious update	1	pyproject.toml

Showing the 60 most significant of 73 distinct findings. The counts in the previous section cover all of them.

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 29 October 2026.