

nextcloud-mcp-server

github.com/cbcoutinho/nextcloud-mcp-server

Scanned 07 October 2026 at 04:52 · Report generated 29 October 2026 · Python · 376 stars

OVERALL ASSESSMENT

Critical

Combined score 552 · 294 findings after filtering

Summary

This repository has two major security issues that are critical to address before anyone can use it. The most serious problem is that the code contains insecure patterns, which means an attacker could exploit these flaws and steal sensitive information or break into the system. Additionally, there are several signs of malicious intent in the code, including suspicious typosquatting and workflows that leak secrets by default. While some findings appear to be ordinary mistakes like logging hardcoded passwords or missing version locks for dependencies, they still represent significant risks because they could lead to credential exposure or supply chain attacks if not fixed. The overall score indicates a high level of vulnerability that requires immediate attention from the developer team to ensure the code is safe and secure.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

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

Critical (531)

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

MALICIOUS PATTERN

Medium (21)

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
semgrep	Insecure coding patterns across many languages	3	159	0	162

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	5	42	48
yara	Signatures of malicious behaviour in source files	5	0	4	9
guarddog	Malicious package and install-time behaviour	0	1	0	1

196 of 294 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	dep_checker	Typosquatting: 'psycopg' is suspiciously similar to 'psycopg2'	1	pyproject.toml
HIGH	semgrep	This workflow uses `secrets: inherit` to pass all of the calling workflow's secrets to a reusable workflow. This violates the principle of least privilege because the called workflow receives access to every secret in the repository, not just the ones it needs. If the called workflow is compromised	1	/.github/workflows/bump-version.yml:130
HIGH	semgrep	Using variable interpolation `\${{...}}` with `github` context data in a `run:` step could allow an attacker to inject their own code into the runner. This would allow them to steal secrets and code. `github` context data can have arbitrary user input and should be treated as untrusted. Instead, use	1	/.github/workflows/pact.yml:86
HIGH	semgrep	Avoiding SQL string concatenation: untrusted input concatenated with raw SQL query can result in SQL Injection. In order to execute raw query safely, prepared statement should be used. SQLAlchemy provides TextualSQL to easily used prepared statement with named parameters. For complex SQL composition	1	/nextcloud_mcp_server/auth/storage.py:1654

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
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/bump-version.yml
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Refresh token stored for user %s (lookup key: %s...)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/browser_oauth_routes.py:613
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Using app password for background sync: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/oauth_sync.py:213
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Username mismatch in app password operation for path user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/api/passwords.py:156
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Stored scoped app password for user %s (scopes=%s, username=%s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:2167
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No app password found for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	2	/nextcloud_mcp_server/auth/storage.py:1942

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Refreshed access token with scopes %s (expires in %ss)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:495
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Refresh token for user %s has expired (expired at %s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:936
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Provisioned app password for user: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/api/passwords.py:520
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "list_tools called - Token type: %s, User scopes: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/app.py:1917
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret " get_provisioning_status: app password FOUND for user_id=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/server/oauth_tools.py:118
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "ingest.skip_no_credentials user=%s doc=%s:%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/queue/procrastinate.py:221

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "[BasicAuth] Removed stale app password for %s after HTTP %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/oauth_sync.py:150
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No refresh token found for user_id=%s (checked provisioning_client_id=%s... and user_id) — " "user completed elicitation but token wasn't stored" being logged. This may lead to secret credentials being exposed. Make sur	1	/nextcloud_mcp_server/server/oauth_tools.py:579
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "[BasicAuth] Periodic cleanup removed %s stale app password(s): %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/oauth_sync.py:523
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "[BasicAuth] No stale app password to remove for %s (HTTP %s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/oauth_sync.py:158
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "[BasicAuth] Failed to remove stale app password for %s: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/vector/oauth_sync.py:164
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "App password for %s is invalid (HTTP %s), removing" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:2072

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Using static OIDC client credentials: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ app.py:1226
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No app password to delete for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ auth/ storage.py:1996
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No access token for %s - allowing (BasicAuth mode)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ auth/ scope_authorization.py:147
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Management API token validated (no audience check) for user: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ auth/ unified_verifier.py:476
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "App password for %s validated (HTTP %s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ auth/ storage.py:2080
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "BasicAuth credentials extracted for user: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/ app.py:844

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Generated background token for user %s with scopes: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:316
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Token refreshed by another thread for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:289
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Failed to get background token for user %s: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:325
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Cleaned up %s stale app password(s): %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/app.py:2453
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Token introspected successfully for user: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/unified_verifier.py:903
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Token found in cache after lock acquisition for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:275

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Retrieved app password for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:1952
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Failed to decrypt app password for user %s: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:1959
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Could not revoke the refused Login Flow app password: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/grant_ownership.py:119
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Retrieved refresh token for user %s (flow_type: %s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:949
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Deleted app password for user: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/api/passwords.py:613
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Deleted app password for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:1989
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Stored app password for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:1899

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Session %s... has no refresh token for user %s; rejecting" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/auth/session_backend.py:100
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No refresh token found for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	3	/ nextcloud_mcp_server/auth/token_broker.py:301
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Stored rotated refresh token for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	2	/ nextcloud_mcp_server/auth/token_broker.py:403
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token refresh failed: %s %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/auth/oauth_routes.py:1539
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Retrieved OAuth client credentials (client_id: %s...)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/auth/storage.py:1320
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token request: grant_type=%s params=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/ nextcloud_mcp_server/auth/oauth_routes.py:1259

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token: client_id mismatch (got=%s, expected=%s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/oauth_routes.py:1382
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token: received code=%s client_id=%s redirect_uri=%s " "code_verifier=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/oauth_routes.py:1328
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token: redirect_uri mismatch (got=%s, expected=%s)" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/oauth_routes.py:1407
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy token: returning IdP token to client %s: refresh_token=%s " "scope=%s expires_in=%s fields=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive inform	1	/nextcloud_mcp_server/auth/oauth_routes.py:1452
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "AS proxy: IdP token response: refresh_token=%s scope=%s expires_in=%s " "token_type=%s fields=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/oauth_routes.py:1154
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "App password cleanup failed (non-fatal): %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/app.py:2459

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Cached token expired for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:59
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Cached token expiring soon for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:64
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Cached token for user %s until %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:80
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "Could not validate app password for %s: %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:2087
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No refresh token to delete for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/storage.py:1101
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No token via provisioning_client_id=%s...; falling back to user_id=%s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/server/oauth_tools.py:560

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	semgrep	Detected a python logger call with a potential hardcoded secret "No refresh token to rotate for user %s" being logged. This may lead to secret credentials being exposed. Make sure that the logger is not logging sensitive information.	1	/nextcloud_mcp_server/auth/token_broker.py:515

Showing the 60 most significant of 211 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 07 October 2026.