



ENGINEERING AUDIT CATALOG

Technical Vulnerability Report

Detailed Code Vulnerability Catalog, Reachability Analysis & Nine-Block Evidence Specification

TARGET SYSTEM & WORKLOAD PROFILE

Target Repository:	CodeSecurity	Monitored Branch:	main
Workload Type:	Infrastructure as Code (IaC / GitOps)	Business Domain:	Information Technology & Cloud SaaS (SOC 2 / ISO 27001)
Project Portfolio:	Production Platform 1320	Scan Execution ID:	#48bb534e

EXECUTIVE POSTURE & GATE SUMMARY

SECURITY POSTURE 100.0 Grade: A	QUALITY GATE PASSED Policy Enforcement	TOTAL FINDINGS 61 Identified Flaws	CRITICAL / HIGH SEVERITY 0 crit • 0 high SLA Action Required
--	---	---	--

ASSESSMENT SCOPE & VERIFIED FRAMEWORKS

Active Inspection Engines: Static Analysis (SAST) • Software Supply Chain (SCA) • Hardcoded Secrets Detection • Infrastructure as Code (IaC) • OWASP Top 10 for LLMs • Dependency Reachability	
Compliance Standards: OWASP Top 10 (2021/2025) • CWE Top 25 • CIS Benchmarks • NIST SP 800-218 (SSDF) • ISO/IEC 27001:2022 • SOC 2 Type II • PCI-DSS v4.0	
Document SHA-256: 23e3b3481279c1ef8a0bab6144ce1d532a1780d378cdb1452fd8bbc51f3619b8	Powered By: Bithost • Licensed By: Zhost Consulting Private Limited
Prepared By: CodeSecurity Autonomous ASPM Engine • Environment: Air-Gapped Verified	© 2026 Zhost Consulting Private Limited. All rights reserved.

ASSESSMENT SCOPE & COVERAGE STATEMENT

Files Scanned: 25 • Files Skipped: 0 • Advisory Freshness: Real-time OSV / NVD / Advisory DB Verified Scan Duration: 146.40s

25 files analyzed across all active detection engines. 0 files excluded from static analysis (0 non-text/binary, 0 vendor/node_modules/cached packages, 0 excluded by .gitignore or file size limit >10MB).

Active Inspection Engines (17): Secret Detection • Python AST SAST • Generic Polyglot SAST • SCA Dependency Auditor • OWASP Top 10 LLM Flaws • License Compliance • IaC Security • Taint Analysis • Dependency Reachability • Container OCI Auditor • Malicious Package Scanner • Supply Chain Provenance • PII Data Privacy • Cryptographic Agility & PQC • Git History Forensics • AI/ML Model Supply Chain • SPDX Source Licensing

SECURITY POSTURE INDEX (SPI) • SCORING & SEVERITY LEDGER

Posture Score = $\max(0.0, 100.0 - \sum (Severity_Base \times Confidence \times EPSS + KEV) \times Tier_Multiplier)$

SEVERITY / FACTOR	ACTIVE COUNT	UNIT PENALTY	NET DEDUCTION	IMPACT & BASIS
Baseline Clean State	—	—	+100.0 pts	Initial pristine benchmark
CRITICAL	0	-30.0 pts	0.0 pts	Immediate exploitability, remote code execution, or exposed credentials
HIGH	0	-12.0 pts	0.0 pts	Privilege escalation, severe injection, or unpatched vulnerable components
MEDIUM	0	-4.5 pts	0.0 pts	Security misconfigurations, weak crypto, or authorization gaps
LOW	0	-0.75 pts	0.0 pts	Hardening opportunities, missing security headers, or hygiene items
Computed Result	61 Flaws	Tier 1 — Mission Critical / Production (1.5× weight)	100.0 / 100.0	Grade A • PASSED GATE

Why Trust This Assessment (Deterministic • Zero AI Hallucination): Deterministic Mathematical Verification: Every point deduction is strictly tied to AST syntax tree violations, CVE/CWE dictionary alignment, and cryptographic commit provenance. Zero AI hallucination or arbitrary score guessing.

Remediation Target: Codebase maintains pristine posture with zero high-severity blockers.

DETAILED FINDING EVIDENCE RECORDS (NINE-BLOCK SPECIFICATION)

LOW High Cyclomatic Complexity (16) in function 'run_staged_scan' SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location: app/services/precommit_hook.py:93

Repository / Target: CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating: HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'run_staged_scan' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001 A.12.6.1 — Management of Technical Vulnerabilities

REMEDIATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.865439

SLA Target: 2026-12-09 17:30:03.861441

LOW

Code Smell: God Function 'generate_pdf' (82 lines)

SQ-SMELL-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/pdf_generator.py:60

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'generate_pdf' exceeds 80 lines of code (82 lines). Break it into smaller, cohesive sub-functions to reduce cognitive load.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.904130

SLA Target: 2026-12-09 17:30:03.902434

LOW

High Cyclomatic Complexity (16) in function 'generate_pdf'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/pdf_generator.py:60

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'generate_pdf' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.910007

SLA Target: 2026-12-09 17:30:03.908999

LOW

High Cognitive Complexity (17) in function 'generate_cyclonedx_json'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/sbom_generator.py:36

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'generate_cyclonedx_json' contains cognitive complexity of 17 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.914093

SLA Target: 2026-12-09 17:30:03.913101

LOW

High Cyclomatic Complexity (16) in function 'build_crsi_explanation'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/report_assembler.py:70

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'build_crsi_explanation' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.917978

SLA Target: 2026-12-09 17:30:03.916095

LOW

High Cyclomatic Complexity (20) in function 'build_nine_block_card'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/report_assembler.py:106

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'build_nine_block_card' contains cyclomatic complexity of 20 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.921462

SLA Target: 2026-12-09 17:30:03.920023

LOW

High Cognitive Complexity (24) in function 'build_nine_block_card'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/report_assembler.py:106

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'build_nine_block_card' contains cognitive complexity of 24 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.923216

SLA Target: 2026-12-09 17:30:03.922571

LOW

High Cyclomatic Complexity (21) in function 'assemble_report_model'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/report_assembler.py:259

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'assemble_report_model' contains cyclomatic complexity of 21 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.928162

SLA Target: 2026-12-09 17:30:03.927160

LOW

High Cognitive Complexity (20) in function 'assemble_report_model'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/report_assembler.py:259

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'assemble_report_model' contains cognitive complexity of 20 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.932059

SLA Target: 2026-12-09 17:30:03.929163

LOW

High Cyclomatic Complexity (17) in function 'dispatch_alert'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/notifier.py:171

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'dispatch_alert' contains cyclomatic complexity of 17 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.934172

SLA Target: 2026-12-09 17:30:03.933164

LOW

High Cognitive Complexity (16) in function 'dispatch_alert'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/notifier.py:171

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'dispatch_alert' contains cognitive complexity of 16 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.936844

SLA Target: 2026-12-09 17:30:03.935171

LOW

Code Smell: Excessive Parameters (6 arguments)

SQ-SMELL-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/audit_verifier.py:14

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function defines 6 parameters. Functions with more than 5 parameters increase coupling and are error-prone. Refactor parameters into a structured configuration object or dataclass.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.937962

SLA Target: 2026-12-09 17:30:03.936844

LOW

Code Smell: God Function 'verify_chain' (100 lines)

SQ-SMELL-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/audit_verifier.py:43

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'verify_chain' exceeds 80 lines of code (100 lines). Break it into smaller, cohesive sub-functions to reduce cognitive load.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.939610

SLA Target: 2026-12-09 17:30:03.939610

LOW

High Cyclomatic Complexity (24) in function 'verify_chain'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/audit_verifier.py:43

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'verify_chain' contains cyclomatic complexity of 24 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.942762

SLA Target: 2026-12-09 17:30:03.941709

LOW

High Cognitive Complexity (23) in function 'verify_chain'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/audit_verifier.py:43

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'verify_chain' contains cognitive complexity of 23 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.944779

SLA Target: 2026-12-09 17:30:03.943717

LOW

High Cyclomatic Complexity (16) in function '_prepare_scan_sandbox'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/services/task_queue.py:136

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function '_prepare_scan_sandbox' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.948651

SLA Target: 2026-12-09 17:30:03.946702

LOW

High Cyclomatic Complexity (16) in function 'run_schema_upgrades'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/models/migration.py:10

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'run_schema_upgrades' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.952253

SLA Target: 2026-12-09 17:30:03.950655

LOW

High Cyclomatic Complexity (22) in function 'login'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/auth.py:30

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'login' contains cyclomatic complexity of 22 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.954330

SLA Target: 2026-12-09 17:30:03.953328

LOW

High Cognitive Complexity (21) in function 'login'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/auth.py:30

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'login' contains cognitive complexity of 21 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.956969

SLA Target: 2026-12-09 17:30:03.955902

LOW

High Cyclomatic Complexity (16) in function 'register'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/auth.py:107

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'register' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.959506

SLA Target: 2026-12-09 17:30:03.957983

LOW

High Cyclomatic Complexity (19) in function 'two_factor_challenge'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/auth.py:252

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'two_factor_challenge' contains cyclomatic complexity of 19 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.962532

SLA Target: 2026-12-09 17:30:03.960533

LOW

High Cognitive Complexity (18) in function 'two_factor_challenge'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/auth.py:252

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'two_factor_challenge' contains cognitive complexity of 18 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.964569

SLA Target: 2026-12-09 17:30:03.963531

LOW

High Cyclomatic Complexity (16) in function 'create_repository'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/repositories.py:42

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'create_repository' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.966573

SLA Target: 2026-12-09 17:30:03.965584

LOW

High Cyclomatic Complexity (25) in function 'ingest_third_party_report'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/api_v1.py:188

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'ingest_third_party_report' contains cyclomatic complexity of 25 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.969197

SLA Target: 2026-12-09 17:30:03.968134

LOW

High Cognitive Complexity (24) in function 'ingest_third_party_report'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/api_v1.py:188

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'ingest_third_party_report' contains cognitive complexity of 24 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.971807

SLA Target: 2026-12-09 17:30:03.970223

LOW

High Cyclomatic Complexity (18) in function 'bulk_triage'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/findings.py:115

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'bulk_triage' contains cyclomatic complexity of 18 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.973834

SLA Target: 2026-12-09 17:30:03.972890

LOW

High Cognitive Complexity (17) in function 'bulk_triage'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/findings.py:115

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'bulk_triage' contains cognitive complexity of 17 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.976846

SLA Target: 2026-12-09 17:30:03.974838

LOW

High Cyclomatic Complexity (19) in function 'triage_finding'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/findings.py:157

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'triage_finding' contains cyclomatic complexity of 19 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.978881

SLA Target: 2026-12-09 17:30:03.976846

LOW

High Cognitive Complexity (18) in function 'triage_finding'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/findings.py:157

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'triage_finding' contains cognitive complexity of 18 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.980883

SLA Target: 2026-12-09 17:30:03.979881

LOW

High Cyclomatic Complexity (16) in function 'index'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/teams.py:20

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'index' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.982836

SLA Target: 2026-12-09 17:30:03.981838

LOW

Code Smell: God Function 'get_openapi_spec' (179 lines)

SQ-SMELL-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/openapi_spec.py:9

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'get_openapi_spec' exceeds 80 lines of code (179 lines). Break it into smaller, cohesive sub-functions to reduce cognitive load.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.985478

SLA Target: 2026-12-09 17:30:03.984354

LOW

High Cognitive Complexity (35) in function 'get_openapi_spec'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/openapi_spec.py:9

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'get_openapi_spec' contains cognitive complexity of 35 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.987468

SLA Target: 2026-12-09 17:30:03.986477

LOW

Code Smell: Deep Control Flow Nesting (depth 5)

SQ-SMELL-03 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/routes/openapi_spec.py:1

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Control flow nesting reaches depth of 5 levels (maximum recommended: 4). Use early returns, guard clauses, or extract helper methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDiation GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.989190

SLA Target: 2026-12-09 17:30:03.988087

LOW

High Cyclomatic Complexity (21) in function 'compare_scans'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/delta_engine.py:66

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'compare_scans' contains cyclomatic complexity of 21 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDIATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.991118

SLA Target: 2026-12-09 17:30:03.990162

LOW

High Cognitive Complexity (20) in function 'compare_scans'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/delta_engine.py:66

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'compare_scans' contains cognitive complexity of 20 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDIATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.993168

SLA Target: 2026-12-09 17:30:03.992146

LOW

High Cyclomatic Complexity (18) in function 'sync_package'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/advisory_sync.py:106

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'sync_package' contains cyclomatic complexity of 18 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.995138

SLA Target: 2026-12-09 17:30:03.994137

LOW

High Cognitive Complexity (17) in function 'sync_package'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/advisory_sync.py:106

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'sync_package' contains cognitive complexity of 17 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:03.997142

SLA Target: 2026-12-09 17:30:03.996134

LOW

High Cyclomatic Complexity (24) in function 'parse_python_file'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/reachability.py:38

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'parse_python_file' contains cyclomatic complexity of 24 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.
Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).
Reachability Status: **UNKNOWN** • CVSS: **0.0** • EPSS Likelihood: **0.0%** • CISA KEV Listed: **NO**

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status:

OPEN

 • First Detected: 2026-09-10 17:30:03.999633

SLA Target: 2026-12-09 17:30:03.998103

LOW

High Cognitive Complexity (23) in function 'parse_python_file'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/reachability.py:38

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'parse_python_file' contains cognitive complexity of 23 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.
Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).
Reachability Status: **UNKNOWN** • CVSS: **0.0** • EPSS Likelihood: **0.0%** • CISA KEV Listed: **NO**

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status:

OPEN

 • First Detected: 2026-09-10 17:30:04.001270

SLA Target: 2026-12-09 17:30:04.000202

LOW

High Cyclomatic Complexity (29) in function 'evaluate_reachability'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/reachability.py:100

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'evaluate_reachability' contains cyclomatic complexity of 29 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.004167

SLA Target: 2026-12-09 17:30:04.002601

LOW

High Cognitive Complexity (28) in function 'evaluate_reachability'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/reachability.py:100

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'evaluate_reachability' contains cognitive complexity of 28 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.006194

SLA Target: 2026-12-09 17:30:04.005192

LOW

High Cyclomatic Complexity (23) in function 'filter_findings'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/suppression.py:103

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'filter_findings' contains cyclomatic complexity of 23 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.008187

SLA Target: 2026-12-09 17:30:04.007191

LOW

High Cognitive Complexity (22) in function 'filter_findings'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/suppression.py:103

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'filter_findings' contains cognitive complexity of 22 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.010198

SLA Target: 2026-12-09 17:30:04.009197

LOW

High Cyclomatic Complexity (25) in function 'is_version_vulnerable'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/semver_matcher.py:55

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'is_version_vulnerable' contains cyclomatic complexity of 25 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.013323

SLA Target: 2026-12-09 17:30:04.012303

LOW

High Cognitive Complexity (24) in function 'is_version_vulnerable'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/semver_matcher.py:55

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'is_version_vulnerable' contains cognitive complexity of 24 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.015349

SLA Target: 2026-12-09 17:30:04.014345

LOW

High Cyclomatic Complexity (19) in function 'evaluate_scan'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/quality_gate.py:19

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'evaluate_scan' contains cyclomatic complexity of 19 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDIATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.016857

SLA Target: 2026-12-09 17:30:04.016345

LOW

High Cognitive Complexity (18) in function 'evaluate_scan'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/quality_gate.py:19

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'evaluate_scan' contains cognitive complexity of 18 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDIATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.019392

SLA Target: 2026-12-09 17:30:04.017874

LOW

High Cyclomatic Complexity (17) in function 'import_sarif'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/sarif.py:31

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'import_sarif' contains cyclomatic complexity of 17 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.021413

SLA Target: 2026-12-09 17:30:04.020414

LOW

High Cognitive Complexity (16) in function 'import_sarif'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/sarif.py:31

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'import_sarif' contains cognitive complexity of 16 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.024415

SLA Target: 2026-12-09 17:30:04.022408

LOW

High Cyclomatic Complexity (39) in function 'auto_detect_format'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/universal_hub.py:34

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'auto_detect_format' contains cyclomatic complexity of 39 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.027823

SLA Target: 2026-12-09 17:30:04.025791

LOW

High Cognitive Complexity (38) in function 'auto_detect_format'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/universal_hub.py:34

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'auto_detect_format' contains cognitive complexity of 38 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.033361

SLA Target: 2026-12-09 17:30:04.030816

LOW

High Cyclomatic Complexity (17) in function 'import_depcheck_xml'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/universal_hub.py:264

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'import_depcheck_xml' contains cyclomatic complexity of 17 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.
Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).
Reachability Status: **UNKNOWN** • CVSS: **0.0** • EPSS Likelihood: **0.0%** • CISA KEV Listed: **NO**

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status:

OPEN

 • First Detected: 2026-09-10 17:30:04.036901

SLA Target: 2026-12-09 17:30:04.034353

LOW

High Cognitive Complexity (16) in function 'import_depcheck_xml'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/scanner/importers/universal_hub.py:264

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'import_depcheck_xml' contains cognitive complexity of 16 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.
Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).
Reachability Status: **UNKNOWN** • CVSS: **0.0** • EPSS Likelihood: **0.0%** • CISA KEV Listed: **NO**

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status:

OPEN

 • First Detected: 2026-09-10 17:30:04.039903

SLA Target: 2026-12-09 17:30:04.037898

LOW

Code Smell: God Function '_handle_tool_call' (137 lines)

SQ-SMELL-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/mcp/server.py:96

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function '_handle_tool_call' exceeds 80 lines of code (137 lines). Break it into smaller, cohesive sub-functions to reduce cognitive load.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.043903

SLA Target: 2026-12-09 17:30:04.040903

LOW

High Cyclomatic Complexity (28) in function '_handle_tool_call'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/mcp/server.py:96

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function '_handle_tool_call' contains cyclomatic complexity of 28 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.045899

SLA Target: 2026-12-09 17:30:04.044902

LOW

High Cognitive Complexity (27) in function '_handle_tool_call'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

app/mcp/server.py:96

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function '_handle_tool_call' contains cognitive complexity of 27 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.048421

SLA Target: 2026-12-09 17:30:04.046901

LOW

High Cyclomatic Complexity (26) in function 'restore_database'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

scripts/restore_db.py:41

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'restore_database' contains cyclomatic complexity of 26 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.050439

SLA Target: 2026-12-09 17:30:04.049438

LOW

High Cognitive Complexity (25) in function 'restore_database'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

scripts/restore_db.py:41

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'restore_database' contains cognitive complexity of 25 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.053716

SLA Target: 2026-12-09 17:30:04.051962

LOW

High Cyclomatic Complexity (21) in function 'main'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

scripts/package_binary.py:39

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'main' contains cyclomatic complexity of 21 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.056751

SLA Target: 2026-12-09 17:30:04.055754

LOW

High Cognitive Complexity (20) in function 'main'

SQ-COMPLEX-02 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

scripts/package_binary.py:39

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'main' contains cognitive complexity of 20 (SonarQube S3776 threshold: 15). Refactor nested control flow to improve readability.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.059761

SLA Target: 2026-12-09 17:30:04.058754

LOW

High Cyclomatic Complexity (16) in function 'build_package'

SQ-COMPLEX-01 | CWE-General • CRSI 5/100

LOCATION & IDENTITY

File Location:

scripts/package_binary.py:116

Repository / Target:

CodeSecurity (branch: main, commit: ed9276da1d)

Confidence Rating:

HIGH

CODE EVIDENCE & VULNERABLE SNIPPET

(No source snippet available)

DESCRIPTION & THREAT IMPACT

Function 'build_package' contains cyclomatic complexity of 16 (SonarQube S1541 threshold: 15). Decompose complex branch trees into smaller cohesive methods.

Business Risk: Impacts CODE_QUALITY posture and confidentiality/integrity.

CONTEXTUAL RISK (CRSI) & REACHABILITY

CRSI 5/100: Base LOW (5) × confidence 1.0 × reachability 1.0 × exploitability 1.00 = 5 (standard baseline rule severity for LOW).

Reachability Status: UNKNOWN • CVSS: 0.0 • EPSS Likelihood: 0.0% • CISA KEV Listed: NO

STANDARDS & REGULATORY CONTROLS ALIGNMENT

ISO IEC 27001

A.12.6.1 — Management of Technical Vulnerabilities

REMEDATION GUIDANCE & FIX (EFFORT: SMALL (<2 H))

Apply the remediation diff or update the affected component.

Status: OPEN • First Detected: 2026-09-10 17:30:04.069825

SLA Target: 2026-12-09 17:30:04.061754



OFFICIAL ATTESTATION OF ASSESSMENT & INTEGRITY

Certificate of Security Posture Verification

This official closing record certifies that the codebase **CodeSecurity** (monitored branch: `main`, commit: `ed9276da1d`) has completed comprehensive automated static security inspection governed by the CodeSecurity Enterprise ASPM engine. The inspection executed across active detection passes covering AST static analysis, polyglot SAST, hardcoded secrets discovery, software supply chain (SCA) vulnerabilities, and infrastructure as code (IaC) misconfigurations under verified, air-gapped deterministic policies.

CRYPTOGRAPHICALLY VERIFIED • TAMPER-PROOF AUDIT RECORD

DOCUMENT PROVENANCE & VERIFICATION

Document SHA-256: `23e3b3481279c1ef8a0bab6144ce1d532a1780d378cdb1452fd8bbc51f3619b8`

Commit Fingerprint: `ed9276da1d8872556e23fef4f5622ad1b6516636`
Scan Execution UUID: `48bb534e-fb84-4899-8991-a273731b9a41`
Audit Integrity Chain: **Append-Only SHA-256 Hash Chain Verified (Law 10 Compliant)**

ENGINE VERSIONS & RULESET PROVENANCE

ENGINE VERSIONS:		RULE-PACK & ADVISORY FEED FRESHNESS:	
AST Static Analysis:	CodeSecurity AST Engine v2.4.0	Universal Rule Pack:	Polyglot 2026.09-REL
Universal Engine:	ContextAware Polyglot Engine v1.8.2	CIS Benchmarks:	v1.6-certified
Secrets & Entropy:	Entropy & Regex Detector v3.1.0	OWASP Standards:	Top10-2021 / LLM-2025
Supply Chain (SCA):	Dependency Advisory Resolver v2.2.0	CWE Dictionary:	CWE-4.14-standard
IaC & CIS Benchmarks:	CIS Benchmark IaC Validator v1.5.0	Threat Intel Feed:	OSV / GitHub Advisory / NVD Realtime Mirror
ASPM Risk Scoring:	Contextual Risk Scoring Engine (CRSI) v2.0	Feed Verification:	✓ VERIFIED AUTHENTIC

REGULATORY FRAMEWORK STANDARDS VERIFIED

OWASP Top 10 2021 / 2025	CWE Top 25 v4.14 Standard	CIS Benchmarks IaC Hardening	NIST SP 800-218 SSDF Compliant
ISO/IEC 27001 Control A.12.6.1	SOC 2 Type II CC6.6 / CC6.8	PCI-DSS v4.0 Requirement 6.2	HIPAA Security 45 CFR §164.312

CodeSecurity Enterprise Application Security Posture Management
Powered By : [Bithost \(www.bithost.in\)](#) | Licensed By: [Zhost Consulting Private Limited](#)
© 2026 Zhost Consulting Private Limited. All rights reserved. Zero-Docker Native Self-Hosted Architecture.

DIGITAL VERIFICATION SIGN-OFF
CodeSecurity Autonomous ASPM
✓ Cryptographically Certified