COMPLIANCE WORKING RECORD

Vulnerability report normalizer

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Document type	Vulnerability report normalizer
Document reference	17-vulnerability-report-normaliser
Jurisdiction	United States
Version	2026-10-09.local-interchange.1
Status	Named review prepared
Prepared by	Fictional Responsible reviewer
Prepared on	October 9, 2026
Generated	October 9, 2026

Purpose and boundary

Combine supported scanner exports into a consistent, source-linked working dataset.

Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Method and exact sources

Method revision 2026-10-09.local-interchange.1.

Read Trivy schemaVersion 2 JSON, Grype matches JSON, or the explicitly documented canonical CSV. Preserve exact scanner IDs, artifact and component versions, vulnerability IDs, source paths and original severity. Normalize only the documented severity labels. Combine both selected sources without deduplication or inferred exploitability. Unsupported structures and incomplete findings remain unresolved.

Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Source	Filename	Bytes	SHA-256
primary	fictional-trivy.json	406	230224c408b46dc7b3e1bc534f2fa9f65defeeaeab07e5dc1586d3c80127545e
comparison	fictional-grype.json	415	a8f7a8af7aeb94d8a0a3dcae673c4336d579073fb1ec7dae8e3f34adf2c1aa7e

Frozen inputs

Field	Value
Review reference	Fictional Review reference
Responsible reviewer	Fictional Responsible reviewer
Observation date	October 9, 2026
Source and version scope	Fictional Source and version scope

Review result

2 source-linked findings. 0 unresolved or failed findings.

- Read Trivy schemaVersion 2 JSON, Grype matches JSON, or the explicitly documented canonical CSV. Preserve exact scanner IDs, artifact and component versions, vulnerability IDs, source paths and original severity. Normalize only the documented severity labels. Combine both selected sources without deduplication or inferred exploitability. Unsupported structures and incomplete findings remain unresolved.

- Original files are unchanged. Working artifacts are separate and withheld when their required checks fail.

Measure	Value
Original files	2
Working artifacts	1
Unresolved findings	0

Normalized scanner findings

The first 25 working rows appear here. Each working preview is limited to 1000 characters. Complete rows and all exact source values remain in Excel and JSON.

Reference	Working result
Trivy schema 2	scanner Trivy schema 2; finding id CVE-2026-00001 / fictional-pkg@1 / 0/0; asset id fictional-image:1; component id fictional-pkg@1; component version 1; vulnerability id CVE-2026-00001; severity High; status affected; source ref /Results/0/Vulnerabilities/0; original severity HIGH; source position Primary / 2
Grype Fictional	scanner Grype Fictional; finding id CVE-2026-00002 / pkg2 / 0; asset id fictional-image:1; component id pkg:npm/fictional-pkg@2; component version 2; vulnerability id CVE-2026-00002; severity Low; status Reported; source ref /matches/0; original severity Low; source position Comparison / 2

Source-linked checks

The formal report shows at most the first 100 named check rows and 400 characters per displayed field. Complete values, result columns, sources and output are retained in the Excel and JSON files.

Unresolved items and limitations

- Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Limitations

- Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Official sources

Source	Provision	Date	Link
RFC Editor: Common Format and MIME Type for CSV Files	Supports CSV interchange only. It specifies no approved domain population, legal criterion or task decision.	October 9, 2026	https://www.rfc-editor.org/rfc/rfc4180