POLARIS INTELLIGENCE

Technical Due Diligence Report

grafana

03 April 2026

Ref: 5e408d8e

CONFIDENTIAL

Heritage Precision Works Ltd trading as Polaris Intelligence
This report is provided for the sole use of the named recipient.

1. Executive Summary

Repository Classification: Production (Confidence: high)
This repository is assessed as production software. All scanner findings are reported at full weight.

Credential/secret findings: 3 critical, 9 findings (4 high confidence). Hardcoded secrets represent immediate exposure risk.

46 known vulnerabilities found in 11 of 1337 dependencies. Outdated or vulnerable packages increase attack surface.

Bus factor: Tier 4: Elevated Concentration. Review recommended to assess key-person dependency.

Malware heuristic scan: 18 heuristic patterns (none high confidence) — manual review recommended. These are heuristic detections — manual review recommended.

4 known supply chain incidents matched against project dependencies (1 sabotage, 1 account_compromise, 1 maintainer_controversy, 1 critical_vulnerability). See Dependencies section for details.

The table below rates risk across 13 dimensions, from Clean (no findings) to Critical (potential deal impact). Together they form the technical risk profile of the target asset.

CATEGORY	RATING	SUMMARY
Secrets & Credentials	CRITICAL RISK	3 critical, 9 findings (4 high confidence)
Dependency Vulnerabilities	CRITICAL RISK	2 critical CVEs
Supply Chain Risk	CRITICAL RISK	2 critical supply chain incidents
Licence & IP	MEDIUM RISK	Project copyleft posture — no third-party contamination detected
Developer Concentration	MEDIUM RISK	Tier 4: Elevated Concentration
Code Quality	CLEAN	Grade B (74.0/100). 28 high-severity potential security anti-patterns warrant review (see Security Anti-Patterns)

CATEGORY	RATING	SUMMARY
Architecture	MEDIUM RISK	23 circular dependencies (0% of modules)
Malware / Destructive Code	MEDIUM RISK	18 heuristic patterns (none high confidence) — manual review recommended
Test Coverage	LOW RISK	Moderate test coverage (26% test ratio, CI gates active) — below comprehensive threshold
Infrastructure & Deployment	LOW RISK	Deployment partially codified — manual steps required
Technical Debt	CLEAN	Minimal tech debt (1828 markers (0.8/KLOC), 2747 suppressions (1.2/KLOC))
Governance & CI/CD	N/A	Not assessed — production repository
Engineering Maturity	LOW RISK	Adequate maturity (30.0 releases/yr, 60% community health)

2. Transaction Impact Assessment

This section translates technical findings into their commercial implications for the transaction. Ratings range from Clean (no concern) to Critical (potential deal-breaker), with specific conditions that may need to be met before or after completion.

CATEGORY	ASSESSMENT	DETAIL
Security Exposure	CRITICAL RISK	3 critical, 9 findings (4 high confidence); 2 critical CVEs; 2 critical supply chain incidents; 18 heuristic patterns (none high confidence) — manual review recommended
Operational Risk	MEDIUM RISK	Tier 4: Elevated Concentration; Grade B (74.0/100). 28 high-severity potential security anti-patterns warrant review (see Security Anti-Patterns)
IP & Licence Risk	MEDIUM RISK	Project copyleft posture — no third-party contamination detected
Integration Complexity	MEDIUM RISK	23 circular dependencies (0% of modules)
Maintenance Burden	MEDIUM RISK	Grade B, 3 quality issues, 1828 tech debt markers

Remediation Effort Estimate

9 critical areas requiring immediate action; 15 high-severity areas for short-term remediation; 57 medium-severity items for the integration roadmap.

Estimates assume a senior developer familiar with the technology stack. Actual effort may vary based on codebase familiarity and organisational context.

3. Scope & Methodology

Repository: https://github.com/grafana/grafana

Analysis date: 03 April 2026

Codebase size: 17,990 files, 4,062,754 lines

LANGUAGE	LINES
TypeScript	1,343,103
Go	1,270,072
JSON	1,189,952
Markdown	163,957
SQL	43,414

Methodology

This report was produced by Polaris Intelligence automated analysis pipeline. The following scanners were applied:

1. **GitHub Enrichment** — project metadata, release cadence, community health
2. **Secret Scanner** — regex pattern matching + context classification
3. **Dependency Scanner** — manifest parsing + OSV vulnerability cross-reference + exploitability analysis
4. **Supply Chain Intelligence** — cross-reference against known supply chain incidents
5. **Licence Auditor** — declared licence + source header contradiction detection
6. **Bus Factor Analysis** — 5-tier developer concentration taxonomy (24-month window)
7. **Code Quality Scorer** — cyclomatic complexity, duplication, security anti-patterns
8. **Architecture Mapper** — import graph, circular dependencies, module coupling
9. **Engineering Maturity** — release discipline, community governance, project signals
10. **Malware Heuristic** — destructive actions, crypto mining, exfiltration, obfuscation

Note: *File counts may vary between sections because each scanner operates on a different subset of files (e.g. quality analysis covers source code files only, while the scope total includes configuration, documentation, and data files).*

This is an automated analysis and does not constitute legal, security, or investment advice. Findings should be verified by qualified professionals.

4. Secrets & Credentials CRITICAL RISK

Hardcoded credentials — API keys, database passwords, tokens — are the most common cause of data breaches. Their presence indicates both an immediate security exposure and a gap in the target's engineering practices that transfers with the acquisition.

9 potential secrets identified — findings include both confirmed exposures and pattern-based detections requiring contextual review:

SEVERITY	CONFIDENCE	CATEGORY	LOCATION	MATCH (REDACTED)
CRITICAL RISK	HIGH	PostgreSQL Connection String	`pkg/services/au...ore/migration/migrator.go:190` [F1]	`connectionStr := fmt.Sprintf("postgresql://***:***@***:***/***",`
MEDIUM RISK	MEDIUM	Password Assignment	`pkg/services/sqlstore/sqlutil/sqlutil.go:165`	`Password: "gra*****est",`
MEDIUM RISK	HIGH	MySQL Connection String	`pkg/storage/uni.../dbimpl/db_engine_test.go:116` [F2]	`require.NoError(t, os.Setenv("GF_DATABASE_URL", "mysql://gf:***@overthere:3306/grafana"))`
CRITICAL RISK	HIGH	PostgreSQL Connection String	`devenv/frontend-service/docker-compose.yaml:38`	`GF_DATABASE_URL: postgres://gra*ana:gra*ana@postgres:5432/gra*ana`
MEDIUM RISK	MEDIUM	Password Assignment	`devenv/docker/b...freeipa/ldap_freeipa.toml:23` [F3]	`bind_password = 'Sec***123'`
MEDIUM RISK	MEDIUM	Password Assignment	`devenv/docker/b...mysql_opendata/Dockerfile:6` [F4]	`MYSQL_ROOT_PASSWORD="roo**ass" \`

SEVERITY	CONFIDENCE	CATEGORY	LOCATION	MATCH (REDACTED)
MEDIUM RISK	MEDIUM	Password Assignment	`devenv/docker/b...luxdb/docker-compose.yaml:11` [F5]	`DOCKER_INFLUXDB_INIT_PASSWORD: 'gra******345'`
MEDIUM RISK	MEDIUM	Generic API Key	`.github/workflows/relyance-scan.yml:30`	`API_KEY: "${{**********...**********}}"`
CRITICAL RISK	HIGH	Private Key (PEM)	`public/app/plug...onfig-v2/AuthSettings.tsx:252` [F6]	`placeholder="Begins with -----BEGIN RSA PRIVATE KEY-----"`

5. Dependency Vulnerabilities CRITICAL RISK

Modern software relies on hundreds of third-party packages. Known vulnerabilities in these dependencies are publicly catalogued and actively exploited. Unpatched critical CVEs represent a quantifiable security liability that transfers to the acquirer.

1337 dependencies analysed across 35 manifests (1083 runtime, 254 dev/test).

46 dependency vulnerabilities found:

Dev vs runtime: *42 in runtime/first-party dependencies, 4 in dev/build-time only.*

SEVERITY		COUNT
CRITICAL	CRITICAL RISK	2
HIGH	HIGH RISK	15
MEDIUM	MEDIUM RISK	28
LOW	LOW RISK	1

SEVERITY	PACKAGE	VERSION	CVE/ ID	SUMMARY	FIX	EXPOSURE
MEDIUM	github.com/ aws/aws- sdk-go	1.55.7	CVE- 2020- 8912	In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/ aws/aws-sdk- go		DECLARED ONLY
MEDIUM (5.0)	github.com/ openfga/ openfga	1.11.3	CVE- 2026- 3372 9	OpenFGA has an Authorization Bypass through cached keys	1.13. 1	DECLARED ONLY
MEDIUM	github.com/ buger/ jsonparser	1.1.2	CVE- 2026- 3228 5	Denial of service in github.com/ buger/ jsonparser		DECLARED ONLY
LOW (7.5)	diff	8.0.0	CVE- 2026- 2400 1	jsdiff has a Denial of Service vulnerability in parsePatch and applyPatch	8.0.3	DECLARED ONLY
MEDIUM (7.5)	js-yaml	4.1.0	CVE- 2025- 6471 8	js-yaml has prototype pollution in merge (<<)	4.1.1	DIRECT IMPORT
MEDIUM (7.5)	lodash	4.17.23	CVE- 2026- 2950	lodash vulnerable to Prototype Pollution via array path bypass in `_.unset` and `_.omit`	4.18. 0	DIRECT IMPORT
HIGH (9.5)	lodash	4.17.23	CVE- 2026- 4800	lodash vulnerable to Code Injection via `_.template` imports key names	4.18. 0	DIRECT IMPORT

SEVERITY	PACKAGE	VERSION	CVE/ ID	SUMMARY	FIX	EXPOSURE
HIGH (7.5)	node-forge	1.3.1	CVE-2026-33896	Forge has a basicConstraints bypass in its certificate chain verification (RFC 5280…	1.4.0	DECLARED ONLY
HIGH (7.5)	node-forge	1.3.1	CVE-2025-66031	node-forge has ASN.1 Unbounded Recursion	1.3.2	DECLARED ONLY
HIGH (9.5)	node-forge	1.3.1	CVE-2025-12816	node-forge has an Interpretation Conflict vulnerability via its ASN.1 Validator…	1.3.2	DECLARED ONLY
MEDIUM (5.0)	yaml	2.0.0	CVE-2026-33532	yaml is vulnerable to Stack Overflow via deeply nested YAML collections	2.8.3	DIRECT IMPORT, DEV
HIGH (7.5)	yaml	2.0.0	CVE-2023-2251	Uncaught Exception in yaml	2.2.2	DIRECT IMPORT, DEV
HIGH (5.0)	github.com/grafana/grafana	inherited	CVE-2020-12458	Grafana information disclosure	7.2.1	DECLARED ONLY
HIGH (5.0)	github.com/grafana/grafana	inherited	CVE-2022-39307	Grafana User enumeration via forget password	9.2.4	DECLARED ONLY
MEDIUM (5.0)	github.com/grafana/grafana	inherited	CVE-2025-3415	Grafana's insecure DingDing Alert integration exposes sensitive information	1.9.2-0.20250514160932-04111e9f2afd	DECLARED ONLY

SEVERITY	PACKAGE	VERSION	CVE/ ID	SUMMARY	FIX	EXPOSURE
HIGH (7.5)	rollup	4.22.4	CVE-2026-27606	Rollup 4 has Arbitrary File Write via Path Traversal	4.59.0	DIRECT IMPORT, DEV
MEDIUM (5.0)	mjml	4.13.0	CVE-2025-67898	MJML allows mj-include directory traversal due to an incomplete fix for CVE-2020-12827		DECLARED ONLY, DEV

First-party packages checked: Go:github.com/grafana/grafana, npm:grafana, Go:github.com/grafana/grafana/pkg/plugins. No known CVEs affecting current version.

Historical CVE Record

These CVEs were filed against prior versions of the target's package. While the current version may not be affected, a history of security incidents indicates recurring risk and may inform the buyer's assessment of the development team's security posture.

github.com/grafana/grafana: 40 CVEs on record

SEVERITY	CVE/ID	SUMMARY
HIGH RISK	CVE-2022-39306	Grafana Email addresses and usernames can not be trusted
MEDIUM RISK	CVE-2023-6152	Email Validation Bypass And Preventing Sign Up From Email's Owner
HIGH RISK	CVE-2020-12458	Grafana information disclosure
HIGH RISK	CVE-2022-39307	Grafana User enumeration via forget password
HIGH RISK	CVE-2025-3260	Grafana vulnerable to authenticated users bypassing dashboard, folder permissions
MEDIUM RISK	CVE-2026-27877	Grafana public dashboards disclose all direct mode datasources
MEDIUM RISK	CVE-2025-3415	Grafana's insecure DingDing Alert integration exposes sensitive information

SEVERITY	CVE/ID	SUMMARY
MEDIUM RISK	CVE-2022-39324	Grafana Spoofing originalUrl of snapshots
MEDIUM RISK	CVE-2019-19499	Grafana Arbitrary File Read
HIGH RISK	CVE-2024-1442	Grafana's users with permissions to create a data source can CRUD all data sources

@grafana/data: 1 CVE on record

SEVERITY	CVE/ID	SUMMARY
MEDIUM RISK	CVE-2021-41174	XSS vulnerability allowing arbitrary JavaScript execution

Supply Chain Intelligence: Dependencies

The following dependencies have a documented history of supply chain incidents — protestware, maintainer sabotage, account compromise, or typosquatting. Even if the current version is safe, the incident history is a material risk signal.

CRITICAL RISK **faker** (npm) — Sabotage

Maintainer (Marak) deleted all code and replaced with 'endgame' message. Same incident as colors.js sabotage.

Date: 2022-01-08 | Current version in repo: 9.8.0 | Incident affected versions: 6.6.6

CRITICAL RISK **eslint-scope** (npm) — Account Compromise

Maintainer's npm credentials stolen via phishing. Malicious version published to steal npm tokens from other developers.

Date: 2018-07-12 | Current version in repo: 8.1.0 | Incident affected versions: 3.7.2

MEDIUM RISK **core-js** (npm) — Maintainer Controversy

Maintainer (zloirock) added donation solicitation messages to install scripts. Critical polyfill depended on by millions of projects, single maintainer with legal issues.

Date: 2023-02-14 | Current version in repo: 3.44.0 | Incident affected versions: 3.x

MEDIUM RISK **lodash** (npm) — Critical Vulnerability

Prototype pollution vulnerabilities discovered repeatedly (CVE-2018-16487, CVE-2019-10744, CVE-2020-28500). Widely depended upon, slow to patch.

Date: 2019-07-02 | Current version in repo: 4.17.20 | Incident affected versions: <4.17.12 | CVE-2019-10744

Dependency Health

"No known CVEs" does not mean healthy dependencies. Stale or abandoned packages receive no security patches and represent latent risk. Health status is derived from package registry release dates.

STATUS		COUNT
Active (released within 6 months)	CLEAN	593
Stable (released within 1 year)	CLEAN	149
Stale (1–2 years since last release)	MEDIUM RISK	169
Abandoned (2+ years since last release)	HIGH RISK	348
Deprecated / Archived	HIGH RISK	9
Unknown (registry lookup failed)	LOW RISK	69

Dependency health score: **6.3/10**

Note: *1 dependency returned implausible release dates from package registries and is excluded from the health score calculation.*

At-Risk Dependencies

PACKAGE	VERSION	STATUS	LAST RELEASE
buf.build/gen/go/parca-dev/parca/connectrpc/go	1.18.1-20250703125925-3f0fcf4bff96.1	HIGH RISK abandoned	0001-01-01 (2025.2yr ago)
buf.build/gen/go/parca-dev/parca/protocolbuffers/go	1.36.2-20250703125925-3f0fcf4bff96.1	HIGH RISK abandoned	0001-01-01 (2025.2yr ago)
github.com/mxk/go-flowrate	0.0.0-20140419014527-cca7078d478f	HIGH RISK abandoned	2014-04-19 (12.0yr ago)
grunt-text-replace	0.4.0	HIGH RISK abandoned	2014-11-23 (11.3yr ago)
github.com/blang/semver	3.5.1+incompatible	HIGH RISK abandoned	2015-02-26 (11.1yr ago)
github.com/yudai/pp	2.0.1+incompatible	HIGH RISK abandoned	2015-03-01 (11.1yr ago)

PACKAGE	VERSION	STATUS	LAST RELEASE
gopkg.in/alexcesaro/quotedprintable.v3	3.0.0-20150716171945-2caba252f4dc	HIGH RISK abandoned	2015-07-16 (10.7yr ago)
github.com/lann/ps	0.0.0-20150810152359-62de8c46ede0	HIGH RISK abandoned	2015-08-10 (10.6yr ago)
github.com/mpvl/unique	0.0.0-20150818121801-cbe035fff7de	HIGH RISK abandoned	2015-08-18 (10.6yr ago)
tween-functions	1.2.0	HIGH RISK abandoned	2015-11-21 (10.3yr ago)
github.com/pmezard/go-difflib	1.0.1-0.20181226105442-5d4384ee4fb2	HIGH RISK abandoned	2016-01-10 (10.2yr ago)
grunt-contrib-copy	1.0.0	HIGH RISK abandoned	2016-03-04 (10.1yr ago)
identity-obj-proxy	3.0.0	HIGH RISK abandoned	2016-08-03 (9.7yr ago)
github.com/valyala/bytebufferpool	1.0.0	HIGH RISK abandoned	2016-08-17 (9.6yr ago)
jsurl	0.1.5	HIGH RISK abandoned	2016-12-07 (9.3yr ago)

Dependency Concentration

High concentration of dependencies from a single namespace increases supply chain risk if that maintainer or organisation is compromised.

NAMESPACE / ORG	DEPENDENCIES
github.com/grafana	66
@types	62
@grafana	33
github.com/aws	28
github.com/hashicorp	26

6. Developer Concentration (Bus Factor) MEDIUM RISK

"Bus factor" measures how many developers would need to leave before critical knowledge is lost. High concentration in one developer creates key-person dependency — a material operational risk that can delay integration and increase post-acquisition costs.

Tier 4: Elevated Concentration — Bus factor score: **49.1%**

49.1% developer concentration across 30 active contributors is above the recommended threshold. While not critical, proactive knowledge sharing is advised to reduce key-person risk.

Top Contributors

DEVELOPER	COMMITS	OWNED FILES	CORE %	STATUS
Ashley Harrison	602	4604	34%	Active
Ryan McKinley	546	968	7%	Active
Stephanie Hingtgen	413	257	1%	Active
Tom Ratcliffe	347	318	2%	Active
Roberto Jiménez Sánchez	339	349	2%	Active
Alexander Akhmetov	282	197	1%	Active
Torkel Ödegaard	256	106	1%	Active
Gilles De Mey	239	215	1%	Active
Yuri Tseretyan	233	175	1%	Active
Matias Chomicki	228	139	1%	Active

Departed Developer Risk

DEVELOPER	MONTHS INACTIVE	CORE FILES OWNED	RISK
Marcus Efraimsson	17	17	HIGH RISK
Diego Augusto Molina	17	14	HIGH RISK
Joao Silva	14	8	HIGH RISK
Scott Lepper	8	7	HIGH RISK
Stijn Van Hoey	7	6	HIGH RISK

DEVELOPER	MONTHS INACTIVE	CORE FILES OWNED	RISK
Alexander Weaver	17	5	MEDIUM RISK
Kristin Laemmert	19	5	MEDIUM RISK
Taewoo K.	10	4	MEDIUM RISK
Giuseppe Guerra	11	4	MEDIUM RISK
Virginia Cepeda	18	4	MEDIUM RISK

7. Licence & Intellectual Property MEDIUM RISK

Copyleft licences (GPL, AGPL) require derivative works to be released under the same open-source terms. If copyleft code is embedded in a proprietary product, the acquirer may face an obligation to open-source their own code — or costly remediation to replace the affected components.

Declared Licences

SPDX ID	RISK	SOURCE	FILE
AGPL-3.0	CRITICAL RISK	licence_file	`LICENSE`
AGPL-3.0	CRITICAL RISK	package_metadata	`package.json`

Project Licensing Posture

The following reflects the project's own chosen licence. This is not contamination — it describes the terms under which this software is distributed.

LICENCE	POSTURE	INVESTOR IMPLICATIONS
AGPL-3.0	Project is licensed under AGPL-3.0 — Network copyleft — all linked/derivative code must be open-sourced under same…	This project is distributed under AGPL-3.0 (network copyleft). Acquirers must comply with copyleft terms or negotiate a commercial licence from the…
AGPL-3.0	Project is licensed under AGPL-3.0 — Network copyleft — all linked/derivative code must be open-sourced under same…	This project is distributed under AGPL-3.0 (network copyleft). Acquirers must comply with copyleft terms or negotiate a commercial licence from the…

No third-party licence contamination detected.

8. Code Quality & Technical Debt CLEAN

Code quality directly predicts the cost and speed of post-acquisition development. A low grade signals elevated technical debt — higher bug rates, slower feature delivery, and more expensive onboarding for new developers joining after the transaction.

Quality grade: **B (74.0/100)** — Acceptable

Note: 28 high security anti-patterns detected — see Security Anti-Patterns below. Grade reflects structural quality only, not security posture.

Grade Scale

GRADE	MEANING
A	Excellent maintainability
B	Good engineering quality
C	Moderate technical debt
D	High technical debt
F	Severe structural risk

METRIC	VALUE
Total files	9616
Code lines	1,103,170
Functions	44265
Classes	7548
Avg function length	17.8 lines
Avg complexity	3.2

Technical Debt Indicators

The following indicators are informational. At this grade level, they represent normal characteristics of a healthy codebase rather than actionable concerns. Duplication above automated thresholds is common in test files and generated code.

- 20 files exceed 500 lines
- 20 functions with high cyclomatic complexity
- Code duplication at 7.4% (threshold: 5.0%)

Complexity Hotspots

SEVERITY	FILE	FUNCTION	COMPLEXITY
HIGH RISK	`public/app/feat...tate/DashboardMigrator.ts` [F7]	updateSchema	204
HIGH RISK	`public/app/plug...tion/statementPosition.ts` [F8]	getStatementPosition	161
HIGH RISK	`apps/plugins/pkg/app/meta/converter.go`	jsonDataToMetaJSONData	142
HIGH RISK	`packages/grafan...lugins/TooltipPlugin2.tsx` [F9]	anonymous	121
HIGH RISK	`pkg/util/xorm/session.go`	slice2Bean	120
HIGH RISK	`public/app/plug.../timeseries/migrations.ts` [F10]	graphToTimeseriesOptions	101
HIGH RISK	`pkg/util/xorm/session_convert.go`	bytes2Value	100
HIGH RISK	`public/app/core...nents/TimeSeries/utils.ts` [F11]	anonymous	97
HIGH RISK	`public/app/core...avBarItem-translations.ts` [F12]	getNavTitle	96
HIGH RISK	`public/app/plugins/panel/barchart/bars.ts`	getConfig	94

Large Files (>500 lines)

FILE	TOTAL LINES	CODE LINES
`packages/grafan...q/legacy/endpoints.gen.ts` [F13]	6206	5614
`packages/grafan...tures/v0alpha1Response.ts` [F14]	4446	4440
`public/app/feat...d/mockGrafanaNotifiers.ts` [F15]	3676	3673
`apps/dashboard/...version/v1_to_v2alpha1.go` [F16]	3139	2434
`pkg/services/featuremgmt/registry.go`	2829	2809
`pkg/apimachinery/utils/meta_mock.go`	2780	2014
`apps/dashboard/...version/v2alpha1_to_v1.go` [F17]	2417	1889

FILE	TOTAL LINES	CODE LINES
`pkg/setting/setting.go`	2416	1788
`pkg/services/da...vice/dashboard_service.go` [F18]	2398	1926
`packages/grafan...v0alpha1/endpoints.gen.ts` [F19]	2230	1520

Security Anti-Patterns

These patterns represent common security vulnerabilities (OWASP Top 10, CWE). Each warrants developer review to confirm whether it represents an actual risk in context.

SEVERITY	PATTERN	LOCATION	DESCRIPTION
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...OperationExplainedBox.tsx:28` [F20]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...ilder/shared/RawQuery.tsx:27` [F21]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...d/OperationInfoButton.tsx:71` [F22]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...nderUserContentAsHTML.tsx:7` [F23]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...peahead/TypeaheadInfo.tsx:46` [F24]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	.innerHTML =	`packages/grafan...explorer/json_explorer.ts:427` [F25]	Direct innerHTML assignment — potential XSS vector
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...NG/Cells/MarkdownCell.tsx:22` [F26]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`packages/grafan...rome/PanelDescription.tsx:26` [F27]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	eval()	`.yarn/releases/yarn-4.11.0.cjs:298`	Dynamic code execution via eval() — potential code injection vector
HIGH RISK	dangerouslySetInnerHTML	`public/app/plug...s2/AnnotationTooltip2.tsx:140` [F28]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement

SEVERITY	PATTERN	LOCATION	DESCRIPTION
HIGH RISK	dangerouslySetInnerHTML	`public/app/plug...AnnotationTooltipBody.tsx:20` [F29]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/plug...l/news/component/News.tsx:48` [F30]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/plug...sQueryEditor/RawQuery.tsx:26` [F31]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/plug...s/prometheus/RawQuery.tsx:24` [F32]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/core...PluginHelp/PluginHelp.tsx:39` [F33]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/core...yListCTA/EmptyListCTA.tsx:64` [F34]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/core...nRow/OperationRowHelp.tsx:31` [F35]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/core/components/help/HelpModal.tsx:257`	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/feat...ailsDeprecatedWarning.tsx:42` [F36]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement
HIGH RISK	dangerouslySetInnerHTML	`public/app/feat...nts/PluginDetailsBody.tsx:57` [F37]	React dangerouslySetInnerHTML — explicit XSS risk acknowledgement

9. Architectural Assessment MEDIUM RISK

10014 production modules (plus 3 test files), 19401 internal dependencies, 6089 external imports.

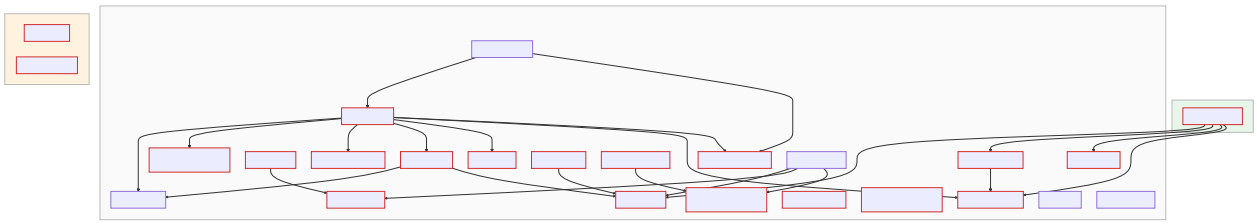
> **23 circular dependencies detected. Circular imports increase coupling and make refactoring more expensive. Breaking these cycles should be prioritised to reduce integration risk.**

Change impact zones: 20 modules have high fan-in (many dependents). Top modules: `pkg/infra/log/databaseQueryTimer.go`, `pkg/setting/setting_grpc.go`, `pkg/apimachinery/identity/static.go`. Changes to these modules carry elevated regression risk.

30 isolated modules detected (no internal imports or dependents). These are typically standalone utilities, examples, platform-specific implementations, or generated code.

Module Dependency Map

Modules are grouped by architectural layer and coloured accordingly. Arrows show import dependencies. Numbers in parentheses indicate how many other modules depend on each file. Thick red borders highlight high fan-in modules (change risk).



Layer Distribution

Modules are grouped by their role in the application: business logic (core functionality), presentation (user-facing), data (storage), and test. A well-structured codebase separates these concerns clearly.

LAYER	MODULES
presentation	5336
other	2787
business_logic	1373
infrastructure	366
data	152

Entry Points (34)

LOCATION	PATTERN
`pkg/cmd/grafana/main.go:24`	`func main(`
`pkg/tsdb/grafan...source/standalone/main.go:10` [F38]	`func main(`
`pkg/tsdb/opentsdb/standalone/main.go:10`	`func main(`
`pkg/tsdb/mssql/standalone/main.go:13`	`func main(`
`pkg/tsdb/loki/standalone/main.go:10`	`func main(`
`pkg/tsdb/grafan...source/standalone/main.go:10` [F39]	`func main(`

LOCATION	PATTERN
`pkg/tsdb/azuremonitor/standalone/main.go:10`	`func main(`
`pkg/tsdb/mysql/standalone/main.go:12`	`func main(`
`pkg/tsdb/graphite/standalone/main.go:10`	`func main(`
`pkg/tsdb/parca/standalone/main.go:10`	`func main(`

Circular Dependencies (23)

`e2e/old-arch/utils/index.ts → e2e/old-arch/utils/support/benchmark.ts → e2e/old-arch/utils/index.ts`

`e2e/old-arch/utils/index.ts → e2e/old-arch/utils/flows/index.ts → e2e/old-arch/utils/flows/addPanel.ts → e2e/old-arch/utils/support/scenarioContext.ts → e2e/old-arch/utils/flows/deleteDataSource.ts → e2e/old-arch/utils/index.ts`

`e2e/old-arch/utils/index.ts → e2e/old-arch/utils/flows/index.ts → e2e/old-arch/utils/flows/addPanel.ts → e2e/old-arch/utils/support/scenarioContext.ts → e2e/old-arch/utils/flows/deleteDashboard.ts → e2e/old-arch/utils/index.ts`

`e2e/old-arch/utils/index.ts → e2e/old-arch/utils/flows/index.ts → e2e/old-arch/utils/flows/addPanel.ts → e2e/old-arch/utils/flows/configurePanel.ts → e2e/old-arch/utils/flows/setTimeRange.ts → e2e/old-arch/utils/flows/selectOption.ts → e2e/old-arch/utils/index.ts`

`e2e/old-arch/utils/index.ts → e2e/old-arch/utils/flows/index.ts → e2e/old-arch/utils/flows/addPanel.ts → e2e/old-arch/utils/flows/configurePanel.ts → e2e/old-arch/utils/flows/setTimeRange.ts → e2e/old-arch/utils/index.ts`

18 additional cycles not shown.

High Fan-In Modules (Change Risk)

"Fan-in" measures how many other parts of the codebase depend on a given file. High fan-in files are widely relied upon — changes to them carry elevated risk because they can affect many dependent components.

MODULE	DEPENDENTS	RISK
`pkg/infra/log/databaseQueryTimer.go`	432	HIGH RISK
`pkg/setting/setting_grpc.go`	385	HIGH RISK

MODULE	DEPENDENTS	RISK
`pkg/apimachinery/identity/static.go`	313	HIGH RISK
`pkg/services/featuremgmt/openfeature.go`	233	HIGH RISK
`pkg/services/ac.../noop_iam_roles_syncer.go` [F40]	216	HIGH RISK
`pkg/apimachinery/utils/resource.go`	177	HIGH RISK
`pkg/util/uri_sanitize.go`	171	HIGH RISK
`pkg/services/ng...s/instance_annotations.go` [F41]	169	HIGH RISK
`apps/provisioni...sioning/v0alpha1/types.go` [F42]	164	HIGH RISK
`pkg/infra/db/sqlbuilder.go`	159	HIGH RISK

Isolated Modules (30)

These files neither use nor are used by any other file in the codebase. They may be unused code, standalone utilities, or components loaded indirectly. Each should be reviewed to confirm it is genuinely needed.

- `.github/actions/report-go-cache-sizes/index.js`
- `.github/workflows/scripts/crowdin/create-tasks.ts`
- `.github/workflows/scripts/json-file-to-job-output.js`
- `.levignore.js`
- `.prettierrc.js`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_client_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_codec_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_object_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_schema_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_spec_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/check_status_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/checktype_client_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/checktype_object_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/checktype_schema_gen.go`
- `apps/advisor/pkg/apis/advisor/v0alpha1/checktype_spec_gen.go`

9b. Architecture Topology

This section applies graph-theoretic analysis to the module dependency network identified in the Architectural Assessment. Community detection reveals natural subsystem boundaries; centrality analysis identifies critical bridge modules whose failure or refactoring would disproportionately affect the codebase.

METRIC	VALUE
Modules analysed	10014
Internal dependencies	19401
Subsystems detected	213
Modularity score	0.794 (strong modular structure)
Unclustered modules	2764

Subsystem Overview

Communities are groups of modules that are more tightly connected to each other than to the rest of the codebase. Each represents a natural subsystem boundary.

SUBSYSTEM	MODULES
packages/ (other, 13 modules)	13
public/app/ (presentation, 438 modules)	438
packages/grafana-flamegraph/ (other, 29 modules)	29
public/app/ (presentation, 95 modules)	95
packages/grafana-i18n/ (other, 6 modules)	6
packages/grafana-api-clients/ (other, 3 modules)	3
scripts/cli/ (other, 5 modules)	5
public/app/ (presentation, 304 modules)	304
public/app/ (presentation, 11 modules)	11
pkg/services/ (business_logic, 109 modules)	109
pkg/ (other, 459 modules)	459
packages/grafana-ui/ (presentation, 2 modules)	2
pkg/tsdb/ (other, 2 modules)	2

SUBSYSTEM	MODULES
packages/grafana-schema/ (other, 7 modules)	7
pkg/ (other, 9 modules)	9

198 additional subsystems not shown.

God Modules (Excessive Coupling)

"God modules" have direct dependencies spanning many subsystems. They violate separation of concerns and make the codebase harder to modify safely — changes risk unintended side effects across multiple subsystems.

MODULE	SUBSYSTEMS	CROSS-EDGES	TOTAL DEGREE	RISK
`pkg/server/wire_gen.go`	4	137	287	HIGH RISK
`pkg/setting/setting_grpc.go`	5	92	385	HIGH RISK
`pkg/infra/log/databaseQueryTimer.go`	5	89	432	HIGH RISK
`pkg/apimachinery/utils/resource.go`	6	88	177	HIGH RISK
`pkg/infra/tracing/tracing_profiling.go`	5	62	159	HIGH RISK
`pkg/apimachinery/identity/static.go`	5	49	313	HIGH RISK
`pkg/services/ac.../noop_iam_roles_syncer.go` [F40]	4	40	216	HIGH RISK
`pkg/services/featuremgmt/openfeature.go`	4	40	235	HIGH RISK
`pkg/infra/db/sqlbuilder.go`	4	31	165	HIGH RISK
`pkg/server/wireexts_oss.go`	3	31	74	HIGH RISK

Package Isolation

Independent packages with zero cross-dependencies. In a monorepo / workspace architecture, this indicates clean separation between packages — a positive architectural signal.

PACKAGE A	PACKAGE B	STATUS
packages/ (other, 13 modules)	public/app/ (presentation, 438 modules)	Independent
packages/ (other, 13 modules)	packages/grafana-flamegraph/ (other, 29 modules)	Independent
packages/ (other, 13 modules)	public/app/ (presentation, 95 modules)	Independent
packages/ (other, 13 modules)	packages/grafana-i18n/ (other, 6 modules)	Independent
packages/ (other, 13 modules)	packages/grafana-api-clients/ (other, 3 modules)	Independent
packages/ (other, 13 modules)	scripts/cli/ (other, 5 modules)	Independent
packages/ (other, 13 modules)	public/app/ (presentation, 304 modules)	Independent
packages/ (other, 13 modules)	public/app/ (presentation, 11 modules)	Independent
packages/ (other, 13 modules)	pkg/services/ (business_logic, 109 modules)	Independent
packages/ (other, 13 modules)	pkg/ (other, 459 modules)	Independent

Structural Gaps

Subsystem pairs with very few connecting dependencies that may indicate missing integration.

SUBSYSTEM A	SUBSYSTEM B	CONNECTING EDGES
public/app/ (presentation, 438 modules)	public/app/ (presentation, 10 modules)	1
public/app/ (presentation, 438 modules)	public/app/ (presentation, 120 modules)	1
public/app/ (presentation, 438 modules)	public/app/ (presentation, 25 modules)	1
public/app/ (presentation, 438 modules)	public/app/ (presentation, 28 modules)	1
public/app/ (presentation, 304 modules)	public/app/ (presentation, 27 modules)	1
public/app/ (presentation, 304 modules)	public/app/ (presentation, 76 modules)	1
public/app/ (presentation, 304 modules)	public/app/ (presentation, 28 modules)	1
pkg/services/ (business_logic, 109 modules)	pkg/ (other, 403 modules)	1

SUBSYSTEM A	SUBSYSTEM B	CONNECTING EDGES
pkg/ (other, 459 modules)	pkg/tsdb/ (other, 17 modules)	1
pkg/ (other, 459 modules)	pkg/generated/ (business_logic, 21 modules)	1

Topology Findings

HIGH RISK **God Module:** Module 'pkg/server/wire_gen.go' connects 4 subsystems with 137 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/setting/setting_grpc.go' connects 5 subsystems with 92 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/infra/log/databaseQueryTimer.go' connects 5 subsystems with 89 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/apimachinery/utils/resource.go' connects 6 subsystems with 88 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/infra/tracing/tracing_profiling.go' connects 5 subsystems with 62 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/apimachinery/identity/static.go' connects 5 subsystems with 49 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/services/accesscontrol/noop_iam_roles_syncer.go' connects 4 subsystems with 40 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/services/featuremgmt/openfeature.go' connects 4 subsystems with 40 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/infra/db/sqlbuilder.go' connects 4 subsystems with 31 cross-boundary edges. Changes here risk cascading across the codebase.

HIGH RISK **God Module:** Module 'pkg/server/wireexts_oss.go' connects 3 subsystems with 31 cross-boundary edges. Changes here risk cascading across the codebase.

LOW RISK **Clean Package Isolation:** 22525 independent package pairs with zero cross-dependencies — clean monorepo isolation.

10. Test Coverage LOW RISK

Automated tests act as safety nets for the codebase. When developers make changes, tests verify nothing else has broken. Strong test coverage means the acquirer's team can modify and extend the code with confidence; weak or absent testing means changes carry a higher risk of introducing undetected problems.

Some testing in place, but gaps remain — coverage is partial or CI enforcement is missing, limiting the safety net for code changes.

The LOW rating reflects CI enforcement uncertainty, not test quality. The test-to-source ratio is above the baseline threshold, indicating meaningful developer investment in testing. The acquirer should verify that CI pipelines enforce test execution on all pull requests.

METRIC	VALUE
Test files	2305
Source files	8858
Test-to-source ratio	26.0%
Test functions / cases	27506

This is a moderate ratio. Some areas of the codebase likely lack test coverage, which increases the cost of making changes safely.

The project uses established testing tools (jest), indicating the team has invested in testing infrastructure.

CI configuration detected *(.github/workflows/backend-unit-tests.yml, .github/workflows/update-schema-types.yml, .github/workflows/migrate-prs.yml, .github/workflows/i18n-crowdin-create-tasks.yml, .github/workflows/release-pr.yml, .github/workflows/detect-breaking-changes-levitate.yml, .github/workflows/feature-toggles-ci.yml, .github/workflows/pr-codeql-analysis-python.yml, .github/workflows/bump-version.yml, .github/workflows/dashboards-issue-add-label.yml, .github/workflows/pr-k8s-codegen-check.yml, .github/workflows/actionlint.yml, .github/workflows/shellcheck.yml, .github/workflows/external-fr-weekly-digest.yml, .github/workflows/swagger-gen.yml, .github/workflows/i18n-verify.yml, .github/workflows/trivy-scan.yml, .github/workflows/stale.yml, .github/workflows/publish-technical-documentation-release.yml, .github/workflows/run-schema-v2-e2e.yml, .github/workflows/pr-commands.yml, .github/workflows/commands.yml, .github/workflows/trufflehog.yml, .github/workflows/github-release.yml, .github/workflows/trigger-dashboard-search-e2e.yml, .github/workflows/pr-codeql-analysis-javascript.yml, .github/workflows/run-dashboard-search-e2e.yml, .github/workflows/community-release.yml, .github/workflows/pr-mt-service-compatibility.yml, .github/workflows/external-pr-notify-handler.yml, .github/workflows/pr-external-labelling.yml, .github/workflows/changelog.yml, .github/workflows/pr-checks.yml, .github/workflows/release-verify.yml, .github/workflows/go-lint.yml, .github/workflows/storybook-a11y.yml, .github/workflows/sync-mirror-event.yml, .github/workflows/add-to-whats-new.yml, .github/workflows/backport-workflow.yml, .github/workflows/pr-patch-check-event.yml, .github/workflows/auto-milestone.yml, .github/workflows/frontend-lint.yml, .github/workflows/pr-go-workspace-check.yml, .github/workflows/release-comms.yml, .github/workflows/analytics-events-report.yml, .github/workflows/pr-dependabot-update-go-workspace.yml, .github/workflows/external-fr-notify.yml, .github/workflows/detect-plugin-extension-changes.yml, .github/workflows/deploy-storybook.yml, .github/workflows/i18n-crowdin-download.yml, .github/workflows/relyance-scan.yml, .github/workflows/alerting-update-module.yml, .github/workflows/backend-code-checks.yml, .github/workflows/publish-technical-documentation-next.yml, .github/workflows/pr-frontend-unit-tests.yml, .github/workflows/skye-add-to-project.yml, .github/workflows/release-build.yml, .github/workflows/release-verify-packages.yml, .github/workflows/issue-opened.yml, .github/workflows/pr-e2e-tests.yml, .github/workflows/deploy-pr-preview.yml, .github/workflows/publish-artifact.yml, .github/workflows/defaults-ini-docs-reminder.yml, .github/workflows/documentation-ci.yml, .github/workflows/backport-trigger.yml, .github/workflows/create-security-patch-from-security-mirror.yml, .github/workflows/pr-build-grafana.yml, .github/workflows/lint-build-docs.yml, .github/workflows/build-go-matrix.yml, .github/workflows/reject-gh-secrets.yml, .github/workflows/frontend-perf-tests.yaml, .github/workflows/externalized-datasources-reminder.yml, .github/workflows/codeowners-validator.yml, .github/workflows/create-next-release-branch.yml, .github/workflows/release-npm.yml, .github/*

workflows/deploy-storybook-preview.yml, .github/workflows/create-security-branch.yml, .github/workflows/external-pr-weekly-digest.yml, .github/workflows/i18n-crowdin-upload.yml, .github/workflows/cleanup-branches.yml, .github/workflows/ephemeral-instances-pr-comment.yml, .github/workflows/pr-test-docker.yml, .github/workflows/codeql-analysis.yml, .github/workflows/pr-patch-check.yml, .github/workflows/check-frontend-test-coverage.yml, .github/workflows/alerting-swagger-gen.yml, .github/workflows/pr-test-integration.yml, .github/workflows/report-frontend-coverage-to-bench.yaml, .github/workflows/external-pr-notify-trigger.yml), but test enforcement could not be fully confirmed. The acquirer should verify that tests run automatically on all pull requests.

11. Infrastructure & Deployment LOW RISK

This section assesses whether the deployment process — how the software is built, packaged, and released — is documented in code or relies on undocumented manual steps. Codified deployment means a new team can operate the software independently; undocumented deployment creates dependency on the original developers and increases transition risk.

Deployment is partially codified — some automation exists but may require manual steps or undocumented knowledge to fully operate.

Deployment is partially codified: CI/CD is present alongside containerisation. A new team would have a reasonable starting point but may need additional context for production deployment.

Infrastructure Found

CATEGORY	TOOLS / CONFIGURATION
Containerisation	dockerfile (25), dockerignore, docker-compose (63)
CI/CD Automation	github-actions (89)

Gaps Identified

- No orchestration (e.g., Kubernetes, Docker Compose) — multi-service deployment is not automated
- No infrastructure-as-code (e.g., Terraform, CloudFormation) — server provisioning may require manual configuration
- No deployment scripts — the release process may rely on undocumented manual steps

12. Technical Debt CLEAN

Technical debt represents shortcuts, deferred work, and known problems that the development team has acknowledged but not yet fixed. Every codebase carries some debt; what matters is the volume and severity. High technical debt increases the cost of post-acquisition development and the risk that changes introduce new problems.

Minimal technical debt — the codebase is well-maintained with few acknowledged shortcuts or deferred work items.

Developers have left **1828** notes in the code flagging work that needs to be done (TODO items, known bugs, temporary workarounds). That is **0.8 markers per 1,000 lines of code**. This density is typical for a well-maintained project.

Debt Markers by Type

TYPE	COUNT
TODO	1448
FIXME	205
HACK	81
WORKAROUND	43
TEMP	35
XXX	16

1464 markers are planned work items (TODO) while 329 flag known problems (FIXME, HACK, BUG). A high proportion of FIXME/HACK markers is more concerning than TODOs, as they indicate acknowledged broken or fragile code.

2747 warning suppressions detected (1.2 per 1,000 lines) — within normal range for a codebase of this size. These represent deliberate exceptions to coding rules, not a material concern.

449 uses of deprecated APIs detected — normal for a mature codebase and not a material risk at current levels.

35 minor error handling patterns detected (empty catch blocks or broad exception handlers) — within normal range and not a material concern at this volume.

13. Engineering Maturity LOW RISK

Engineering maturity measures the project's operational health beyond source code quality — release discipline, community governance, and project signals that indicate long-term viability.

Overall maturity: **B** — minor maturity gaps only (risk rating: LOW)

Release Cadence

METRIC	VALUE
Releases per year	30

METRIC	VALUE
Days since last release	8
Semver compliance	100.0%
Grade	A

Community Health

DOCUMENT	STATUS
SECURITY.md	Missing
CONTRIBUTING.md	Present
CODE_OF_CONDUCT	Present
Issue template	Missing
PR template	Present
Health score	60%
Grade	C

Project Signals

METRIC	VALUE
Stars	72,946
Forks	13,657
Open issues	3,928
Contributors	100
Repository created on GitHub	2013-12-11
Grade	A

Note: *GitHub API reports 100 contributors while git history analysis (Bus Factor section) identified 30. This discrepancy arises because GitHub counts all commit authors across the full history, while git analysis may use a limited clone depth or different author-deduplication rules.*

14. Malware & Destructive Action Scan MEDIUM RISK

This scan searches for code patterns commonly associated with protestware, supply-chain attacks, and sabotage — filesystem wipers, obfuscated payloads, unauthorised network calls, and install-hook abuse. Findings are heuristic and warrant manual review rather than automatic condemnation.

Files scanned: 14,457

18 heuristic patterns detected — these are common in legitimate code (build scripts, test harnesses, networking libraries) and do not indicate malicious intent without manual verification.

CATEGORY	FINDINGS
Filesystem Destruction	1
Network Exfiltration	8
Process Execution	9

SEVERITY	CONFIDENCE	LOCATION	PATTERN	CODE
CRITICAL RISK	MEDIUM	`devenv/bulk-folders/bulk-folders.sh:4`	Recursive force deletion (rm -rf)	`find ./bulk-folders -type d -name "Bulk Folder*" -exec rm -r`
MEDIUM RISK	MEDIUM	`scripts/levitate-show-affected-plugins.js:7`	Importing child_process module (Node.js)	`const { execSync } = require('child_process');`
HIGH RISK	MEDIUM	`scripts/test-coverage-by-codeowner.js:38`	Process execution via child_process (Node.js)	`const child = cp.spawn('jest', [`--config=${JEST_CONFIG_PATH`
HIGH RISK	MEDIUM	`packages/grafan...formers/joinDataFrames.ts:419` [F43]	Dynamic function creation via new Function() (JavaScript)	`let materialize = new Function(`
HIGH RISK	MEDIUM	`packages/grafan...ces/pluginMeta/plugins.ts:19` [F44]	HTTP request with dynamic URL (potential data exfiltration)	`const metas = await fetch(`apis/plugins.grafana.app/${getApi`

SEVERITY	CONFIDENCE	LOCATION	PATTERN	CODE
HIGH RISK	MEDIUM	`packages/grafan....app/v0alpha1/handlers.ts:71` [F45]	HTTP request with dynamic URL (potential data exfiltration)	`const settingsHandler = (response = defaultSettings) => http`
HIGH RISK	MEDIUM	`packages/grafan....app/v0alpha1/handlers.ts:59` [F46]	HTTP request with dynamic URL (potential data exfiltration)	`http.get(`${API_BASE}/find/scope_node_childre n`, ({ request`
HIGH RISK	MEDIUM	`packages/grafan...ts/Table/TableNG/utils.ts:821` [F47]	Dynamic function creation via new Function() (JavaScript)	`return new Function('frame', 'nestedRowIndex', fnBody) as Fr`
HIGH RISK	MEDIUM	`packages/grafan...eNG/Filter/FilterList.tsx:70` [F48]	Dynamic function creation via new Function() (JavaScript)	`const fnc = new Function('$', `'use strict'; return ${xpr};`
HIGH RISK	MEDIUM	`packages/grafan...le/TableRT/FilterList.tsx:102` [F49]	Dynamic function creation via new Function() (JavaScript)	`const fnc = new Function('$', `'use strict'; return ${xpr};`
HIGH RISK	MEDIUM	`public/app/plugins/panel/xychart/scatter.ts:672`	Dynamic function creation via new Function() (JavaScript)	`getOne = new Function('v', `return ${conds};`) as GetOneValu`
HIGH RISK	MEDIUM	`public/app/plug...yers/basemaps/maplibre.ts:70` [F50]	HTTP request with dynamic URL (potential data exfiltration)	`const res = await fetch(cfg.url);`
HIGH RISK	MEDIUM	`public/app/core/services/context_srv.ts:252`	HTTP request with dynamic URL (potential data exfiltration)	`return fetch(config.appSubUrl + '/api/user/auth-tokens/rotat`
HIGH RISK	MEDIUM	`public/app/feat...erting/unified/mockApi.ts:175` [F51]	HTTP request with dynamic URL (potential data exfiltration)	`http.get(`api/prometheus/${dsName}/api/v1/rules`, () => Http`

SEVERITY	CONFIDENCE	LOCATION	PATTERN	CODE
HIGH RISK	MEDIUM	`public/app/feat...ces/DashboardLoaderSrv.ts:76` [F52]	Dynamic function creation via new Function() (JavaScript)	`const scriptFunc = new Function(`
HIGH RISK	MEDIUM	`public/app/feat...munityDashboardHelpers.ts:181` [F53]	Dynamic function creation via new Function() (JavaScript)	`/\bnew\s+Function\s*\(/i, // new Function() constructor`
HIGH RISK	MEDIUM	`public/app/feat.../editors/FileUploader.tsx:48` [F54]	HTTP request with dynamic URL (potential data exfiltration)	`fetch(`/api/storage/delete/upload/${file.file.name}`, {`
HIGH RISK	MEDIUM	`public/swagger/K8sNameLookup.tsx:37`	HTTP request with dynamic URL (potential data exfiltration)	`const response = await fetch(url + '?limit=100', {`

15. Risk Summary & Recommendations

Recommendations are prioritised by their potential impact on the transaction. Immediate and Urgent items should be addressed as conditions precedent; Medium items can be scheduled into the post-acquisition integration roadmap.

PRIORITY	CATEGORY	RECOMMENDED ACTION
CRITICAL RISK	Secrets & Credentials	Rotate all detected credentials and remove from source code. Implement secrets management (e.g., HashiCorp Vault, AWS Secrets Manager).
URGENT	Dependency Vulnerabilities	Patch 2 critical CVEs immediately. Update pinned dependency versions.
URGENT	Supply Chain Risk	4 dependencies have documented supply chain incidents. Review affected packages, pin to known-safe versions, and consider alternatives.
HIGH RISK	Licence Risk	Engage legal counsel to assess copyleft exposure and implications for the acquirer's intended use.
MEDIUM RISK	Dependency Health	357 abandoned or deprecated dependencies. Evaluate alternatives to reduce latent supply chain risk.

Appendix A: Raw Data

Dependency Inventory (1337 packages)

ECOSYSTEM	PACKAGE	VERSION	VULNS	HEALTH	LAST RELEASE
Go	buf.build/gen/go/parca-dev/parca/connectrpc/go	1.18.1-20250703125925-3f0fcf4bff96.1	0	abandoned	0001-01-01
Go	buf.build/gen/go/parca-dev/parca/protocolbuffers/go	1.36.2-20250703125925-3f0fcf4bff96.1	0	abandoned	0001-01-01
Go	cloud.google.com/go/kms	1.25.0	0	active	2026-02-19
Go	cloud.google.com/go/storage	1.56.0	0	active	2026-03-13
Go	connectrpc.com/connect	1.19.1	0	active	2025-10-07
Go	dario.cat/mergo	1.0.2	0	stable	2025-05-07
Go	filippo.io/age	1.2.1	0	active	2025-12-28
Go	github.com/1NCE-GmbH/grpc-go-pool	0.0.0-20231117122434-2a5bb974daa2	0	unknown	
Go	github.com/Azure/azure-sdk-for-go	68.0.0+incompatible	0	unknown	
Go	github.com/Azure/azure-sdk-for-go/sdk/azcore	1.20.0	0	unknown	
Go	github.com/Azure/azure-sdk-for-go/sdk/azidentity	1.13.1	0	unknown	
Go	github.com/Azure/azure-sdk-for-go/sdk/keyvault/azkeys	0.10.0	0	unknown	
Go	github.com/Azure/azure-storage-blob-go	0.15.0	0	unknown	
Go	github.com/Azure/go-autorest/autorest	0.11.30	0	unknown	
Go	github.com/Azure/go-autorest/autorest/adal	0.9.24	0	unknown	
Go	github.com/Bose/minisentinel	0.0.0-20200130220412-917c5a9223bb	0	unknown	
Go	github.com/BurntSushi/toml	1.5.0	0	unknown	
Go	github.com/DATA-DOG/go-sqlmock	1.5.2	0	unknown	
Go	github.com/Masterminds/semver	1.5.0	0	unknown	
Go	github.com/Masterminds/semver/v3	3.4.0	0	unknown	
Go	github.com/Masterminds/sprig/v3	3.3.0	0	unknown	
Go	github.com/VividCortex/mysqlerr	1.0.0	0	unknown	

ECOSYSTEM	PACKAGE	VERSION	VULNS	HEALTH	LAST RELEASE
Go	github.com/alicebob/miniredis/v2	2.34.0	0	active	2026-02-25
Go	github.com/andybalholm/brotli	1.2.0	0	active	2026-03-24
Go	github.com/apache/arrow-go/v18	18.5.2	0	active	2026-02-27
Go	github.com/armon/go-radix	1.0.0	0	abandoned	2018-08-24
Go	github.com/aws/aws-sdk-go	1.55.7	1	stable	2025-07-31
Go	github.com/aws/aws-sdk-go-v2	1.41.1	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/credentials	1.19.7	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/cloudwatch	1.45.3	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/cloudwatchlogs	1.51.0	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/ec2	1.225.2	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/oam	1.18.3	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/resourcegroupstaggingapi	1.26.6	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/secretsmanager	1.40.1	0	active	2026-03-26
Go	github.com/aws/aws-sdk-go-v2/service/sts	1.41.6	0	active	2026-03-26
Go	github.com/aws/smithy-go	1.24.0	0	active	2026-02-27
Go	github.com/beevik/etree	1.6.0	0	stable	2025-08-22
Go	github.com/benbjohnson/clock	1.3.5	0	abandoned	2023-05-18
Go	github.com/blevesearch/bleve/v2	2.5.7	0	active	2025-12-15
Go	github.com/blevesearch/bleve_index_api	1.3.0	0	active	2026-03-26
Go	github.com/bradfitz/gomemcache	0.0.0-20250403215159-8d39553ac7cf	0	stable	2025-04-03
Go	github.com/bwmarrin/snowflake	0.3.0	0	abandoned	2019-04-12
Go	github.com/centrifugal/centrifuge	0.38.0	0	active	2025-11-14
Go	github.com/crewjam/saml	0.4.14	0	stable	2025-04-14
Go	github.com/dgraph-io/badger/v4	4.9.1	0	active	2026-02-04
Go	github.com/dlmiddlecote/sqlstats	1.0.2	0	abandoned	2021-02-08
Go	github.com/docker/go-connections	0.6.0	0	stable	2025-08-06
Go	github.com/dolthub/go-mysql-server	0.19.1-0.20250410182021-5632d67cd46e	0	stable	2025-05-13

ECOSYSTEM	PACKAGE	VERSION	VULNS	HEALTH	LAST RELEASE
Go	github.com/dolthub/vitess	0.0.0-20260225173707-20566e4abe9e	0	abandoned	2017-05-22
Go	github.com/dustin/go-humanize	1.0.1	0	abandoned	2023-01-10
Go	github.com/emicklei/go-restful/v3	3.13.0	0	stable	2025-08-14
Go	github.com/fatih/color	1.18.0	0	active	2026-03-20
Go	github.com/fullstorydev/grpchan	1.1.1	0	active	2025-10-29
Go	github.com/gchaincl/sqlhooks	1.3.0	0	abandoned	2019-11-25
Go	github.com/getkin/kin-openapi	0.134.0	0	active	2026-03-13
Go	github.com/go-jose/go-jose/v4	4.1.4	0	active	2025-10-03
Go	github.com/go-kit/log	0.2.1	0	abandoned	2022-04-27
Go	github.com/go-ldap/ldap/v3	3.4.4	0	active	2026-03-01
Go	github.com/go-logfmt/logfmt	0.6.1	0	active	2025-10-05
Go	github.com/go-openapi/loads	0.23.3	0	active	2026-03-08
Go	github.com/go-openapi/runtime	0.28.0	0	active	2026-03-08
Go	github.com/go-openapi/strfmt	0.26.0	0	active	2026-03-15
Go	github.com/go-sourcemap/sourcemap	2.1.4+incompatible	0	abandoned	2024-03-13
Go	github.com/go-sql-driver/mysql	1.9.3	0	stable	2025-06-13
Go	github.com/go-stack/stack	1.8.1	0	abandoned	2021-08-18
Go	github.com/gobwas/glob	0.2.3	0	abandoned	2018-02-08
Go	github.com/gogo/protobuf	1.3.2	0	abandoned	2021-01-10
Go	github.com/golang-jwt/jwt/v4	4.5.2	0	stale	2025-03-21
Go	github.com/golang-migrate/migrate/v4	4.7.0	0	active	2025-11-29
Go	github.com/golang/mock	1.7.0-rc.1	0	abandoned	2021-06-11
Go	github.com/golang/protobuf	1.5.4	0	abandoned	2024-03-06
Go	github.com/golang/snappy	1.0.0	0	abandoned	2023-12-25
Go	github.com/google/go-cmp	0.7.0	0	stale	2025-01-14
Go	github.com/google/go-github/v82	82.0.0	0	active	2026-01-27
Go	github.com/google/uuid	1.6.0	0	abandoned	2024-01-23
Go	github.com/google/wire	0.7.0	0	stable	2025-08-22
Go	github.com/googleapis/gax-go/v2	2.15.0	0	active	2026-04-01
Go	github.com/gorilla/mux	1.8.1	0	abandoned	2023-10-18
Go	github.com/gorilla/websocket	1.5.4-0.20250319132907-e064f32e3674	0	stale	2024-06-14
Go	github.com/grafana/alerting	0.0.0-20260330164719-5946ccd00861	0	active	2026-03-27

ECOSYSTEM	PACKAGE	VERSION	VULNS	HEALTH	LAST RELEASE
Go	github.com/grafana/authlib	0.0.0-20260316143530-e1d123886039	0	active	2026-03-16
Go	github.com/grafana/authlib/types	0.0.0-20260316143530-e1d123886039	0	active	2026-03-16
Go	github.com/grafana/dataplane/examples	0.0.1	0	abandoned	2023-07-13
Go	github.com/grafana/dataplane/sdata	0.0.9	0	stale	2024-04-16
Go	github.com/grafana/dskit	0.0.0-20260108123158-1a1acfb6ef2e	0	active	2026-03-26
Go	github.com/grafana/e2e	0.1.1	0	abandoned	2023-09-19
Go	github.com/grafana/gofpdf	0.0.0-20250307124105-3b9c5d35577f	0	active	2025-11-24
Go	github.com/grafana/gomemcache	0.0.0-20251127154401-74f93547077b	0	active	2025-11-27
Go	github.com/grafana/grafana-api-golang-client	0.27.0	0	abandoned	2023-12-11
Go	github.com/grafana/grafana-app-sdk	0.52.1	0	active	2026-03-20
Go	github.com/grafana/grafana-app-sdk/logging	0.51.4	0	active	2026-03-20
Go	github.com/grafana/grafana-aws-sdk	1.4.3	0	active	2026-01-29
Go	github.com/grafana/grafana-azure-sdk-go/v2	2.4.0	0	active	2026-02-20
Go	github.com/grafana/grafana-cloud-migration-snapshot	1.10.0	0	active	2026-02-06
Go	github.com/grafana/grafana-google-sdk-go	0.4.2	0	stable	2025-08-01
Go	github.com/grafana/grafana-openapi-client-go	0.0.0-20231213163343-bd475d63fb79	0	active	2025-12-02
Go	github.com/grafana/grafana-plugin-sdk-go	0.291.0	0	active	2026-03-11
Go	github.com/grafana/loki/pkg/push	0.0.0-20250823105456-332df2b20000	0	active	2026-03-27
Go	github.com/grafana/loki/v3	3.5.11	0	active	2026-03-26

Module Dependencies (top 30)

MODULE	FAN-IN	LAYER
`pkg/infra/log/databaseQueryTimer.go`	432	other

MODULE	FAN-IN	LAYER
`pkg/setting/setting_grpc.go`	385	other
`pkg/apimachinery/identity/static.go`	313	other
`pkg/services/featuremgmt/openfeature.go`	233	business_logic
`pkg/services/ac.../noop_iam_roles_syncer.go` [F40]	216	business_logic
`pkg/apimachinery/utils/resource.go`	177	infrastructure
`pkg/util/uri_sanitize.go`	171	infrastructure
`pkg/services/ng...s/instance_annotations.go` [F41]	169	business_logic
`apps/provisioni...sioning/v0alpha1/types.go` [F42]	164	other
`pkg/infra/db/sqlbuilder.go`	159	data
`pkg/infra/tracing/tracing_profiling.go`	159	other
`pkg/services/contexthandler/model/model.go`	149	business_logic
`pkg/services/user/user.go`	137	business_logic
`pkg/services/org/model.go`	126	business_logic
`pkg/plugins/plugins.go`	121	other
`pkg/services/datasources/accesscontrol.go`	119	business_logic
`public/app/feat...oard-scene/utils/utils.ts` [F55]	114	presentation
`public/app/feat...ified/utils/datasource.ts` [F56]	112	presentation
`pkg/web/response_writer.go`	112	other
`pkg/services/sqlstore/migrator/testing.go`	110	business_logic
`pkg/api/response/web_hack.go`	101	other
`pkg/services/dashboards/dashboard.go`	97	business_logic
`pkg/apimachinery/errutil/template.go`	96	other
`pkg/services/ng...ooling/definitions/api.go` [F57]	88	business_logic
`packages/grafana-data/src/types/dataFrame.ts`	88	other
`pkg/services/ap...ints/request/namespace.go` [F58]	83	business_logic
`public/app/feat...ing/unified/utils/misc.ts` [F59]	81	presentation
`public/app/feat...ng/unified/utils/rules.ts` [F60]	80	presentation
`apps/provisioning/pkg/repository/tester.go`	76	other
`pkg/storage/unified/resource/errors.go`	71	other

Appendix B: File Reference

Full file paths for truncated references in the report.

REF	FULL PATH
F1	`pkg/services/authz/zanzana/store/migration/migrator.go`
F2	`pkg/storage/unified/sql/db/dbimpl/db_engine_test.go`
F3	`devenv/docker/blocks/auth/freeipa/ldap_freeipa.toml`
F4	`devenv/docker/blocks/mysql_opendata/Dockerfile`
F5	`devenv/docker/blocks/influxdb/docker-compose.yaml`
F6	`public/app/plugins/datasource/influxdb/components/editor/config-v2/AuthSettings.tsx`
F7	`public/app/features/dashboard/state/DashboardMigrator.ts`
F8	`public/app/plugins/datasource/cloudwatch/language/cloudwatch-logs-sql/completion/statementPosition.ts`
F9	`packages/grafana-ui/src/components/uPlot/plugins/TooltipPlugin2.tsx`
F10	`public/app/plugins/panel/timeseries/migrations.ts`
F11	`public/app/core/components/TimeSeries/utils.ts`
F12	`public/app/core/utils/navBarItem-translations.ts`
F13	`packages/grafana-api-clients/src/clients/rtkq/legacy/endpoints.gen.ts`
F14	`packages/grafana-runtime/src/services/pluginMeta/test-fixtures/v0alpha1Response.ts`
F15	`public/app/features/alerting/unified/mockGrafanaNotifiers.ts`
F16	`apps/dashboard/pkg/migration/conversion/v1_to_v2alpha1.go`
F17	`apps/dashboard/pkg/migration/conversion/v2alpha1_to_v1.go`
F18	`pkg/services/dashboards/service/dashboard_service.go`
F19	`packages/grafana-api-clients/src/clients/rtkq/provisioning/v0alpha1/endpoints.gen.ts`
F20	`packages/grafana-prometheus/src/querybuilder/shared/OperationExplainedBox.tsx`
F21	`packages/grafana-prometheus/src/querybuilder/shared/RawQuery.tsx`
F22	`packages/grafana-prometheus/src/querybuilder/shared/OperationInfoButton.tsx`
F23	`packages/grafana-ui/src/components/RenderUserContentAsHTML/RenderUserContentAsHTML.tsx`
F24	`packages/grafana-ui/src/components/Typeahead/TypeaheadInfo.tsx`
F25	`packages/grafana-ui/src/components/JSONFormatter/json_explorer/json_explorer.ts`
F26	`packages/grafana-ui/src/components/Table/TableNG/Cells/MarkdownCell.tsx`
F27	`packages/grafana-ui/src/components/PanelChrome/PanelDescription.tsx`
F28	`public/app/plugins/panel/timeseries/plugins/annotations2/AnnotationTooltip2.tsx`
F29	`public/app/plugins/panel/timeseries/plugins/annotations2-cluster/AnnotationTooltipBody.tsx`
F30	`public/app/plugins/panel/news/component/News.tsx`
F31	`public/app/plugins/datasource/azuremonitor/components/LogsQueryEditor/RawQuery.tsx`

REF	FULL PATH
F32	`public/app/plugins/datasource/tempo/_importedDependencies/datasources/prometheus/RawQuery.tsx`
F33	`public/app/core/components/PluginHelp/PluginHelp.tsx`
F34	`public/app/core/components/EmptyListCTA/EmptyListCTA.tsx`
F35	`public/app/core/components/QueryOperationRow/OperationRowHelp.tsx`
F36	`public/app/features/plugins/admin/components/PluginDetailsDeprecatedWarning.tsx`
F37	`public/app/features/plugins/admin/components/PluginDetailsBody.tsx`
F38	`pkg/tsdb/grafana-testdata-datasource/standalone/main.go`
F39	`pkg/tsdb/grafana-pyroscope-datasource/standalone/main.go`
F40	`pkg/services/accesscontrol/noop_iam_roles_syncer.go`
F41	`pkg/services/ngalert/models/instance_annotations.go`
F42	`apps/provisioning/pkg/apis/provisioning/v0alpha1/types.go`
F43	`packages/grafana-data/src/transformations/transformers/joinDataFrames.ts`
F44	`packages/grafana-runtime/src/services/pluginMeta/plugins.ts`
F45	`packages/grafana-test-utils/src/handlers/apis/provisioning.grafana.app/v0alpha1/handlers.ts`
F46	`packages/grafana-test-utils/src/handlers/apis/scope.grafana.app/v0alpha1/handlers.ts`
F47	`packages/grafana-ui/src/components/Table/TableNG/utils.ts`
F48	`packages/grafana-ui/src/components/Table/TableNG/Filter/FilterList.tsx`
F49	`packages/grafana-ui/src/components/Table/TableRT/FilterList.tsx`
F50	`public/app/plugins/panel/geomap/layers/basemaps/maplibre.ts`
F51	`public/app/features/alerting/unified/mockApi.ts`
F52	`public/app/features/dashboard/services/DashboardLoaderSrv.ts`
F53	`public/app/features/dashboard/dashgrid/DashboardLibrary/utils/communityDashboardHelpers.ts`
F54	`public/app/features/dimensions/editors/FileUploader.tsx`
F55	`public/app/features/dashboard-scene/utils/utils.ts`
F56	`public/app/features/alerting/unified/utils/datasource.ts`
F57	`pkg/services/ngalert/api/tooling/definitions/api.go`
F58	`pkg/services/apiserver/endpoints/request/namespace.go`
F59	`public/app/features/alerting/unified/utils/misc.ts`
F60	`public/app/features/alerting/unified/utils/rules.ts`