@FOLIO_LSP

FOLIO

*The Future of Libraries is Open*

# FOLIO Security Team Overview

Craig McNally | September 23, 2025

# Agenda

- What is the Security Team?
  - Who is on the Security Team?
  - What do we do?
- How do we learn of vulnerabilities?
  - Types of scans/analysis/testing in use
- Vulnerability lifecycle and Workflows
  - Severe/Critical issues
  - Responsible Disclosure
  - False Alarms
- How can we improve FOLIO Security?
  - Careful with AI-Generated Code!
  - Dashboarding Initiative
- Additional Info
- Questions?

https://deepai.org/

# What is the Folio Security Team?

The FOLIO Security Team consists of a group of individuals who volunteered to **oversee the identification and resolution of security vulnerabilities reported against FOLIO**. The FOLIO Security Team works in close collaboration with the Technical Council and the development team of the affected component. The composition of the Security Team is determined by the FOLIO project governance bodies.

# What is the FOLIO Security Team?

## Active team members:

- Craig McNally (EBSCO)
  - Unofficial convener
- Julian Ladisch (GBV)
- Jens Heinrich (Frankfurt University Library)
- Ryan Berger (EBSCO)
- Chris Rutledge (Texas A&M)
- Kevin Day (Texas A&M)
- John Coburn (EBSCO)

# What is the FOLIO Security Team?

## What do we do?

Official responsibilities:

1. Triage reported security vulnerabilities
2. Manage the lifecycle of identified security vulnerabilities
3. Provide appropriate notifications to the Folio community and broader public.

Unofficial/Voluntary responsibilities (Time Permitting):

1. Ad-hoc/manual (proactive) scanning and monitoring
2. Provide security advice/guidance to development teams/councils
3. Draft security-related policy proposals

# How do we learn about vulnerabilities?

## Types of scans/analysis/testing in use:

### Software Composition Analysis (SCA)

Analyzes codebases, and binaries (e.g. docker images). Identifies vulnerabilities in third party software. Sometimes also can analyze license compliance.

### Static Application Security Testing (SAST)

Analyzes source code, identifying vulnerabilities like XSS, SQL injection, hardcoded secrets, etc.

### Dynamic Application Security Testing (DAST)

Simulates real-world attacks against software at runtime. Sometimes referred to as “Blackbox testing”.

### Penetration Testing (Pen testing)

Security professionals attempt to exploit vulnerabilities in your application at runtime.

# How do we learn about vulnerabilities?

**Reported by the community, word of mouth, blogs, etc.**

- Safe Harbor Statement

**Folio project tooling**

- Snyk (continuous – SAST/SCA)
- Semgrep (continuous – SAST/SCA)
- SonarQube (continuous - SAST)
- GitHub advisories, secret scans (continuous - SCA)
- ZAP/OWASP top 10 scans (manual, periodic - DAST)

**External**

- Penetration testing (EBSCO)
- PRISMA scans (EBSCO/FSE - SCA)






# Vulnerability Lifecycle / Workflows

- **Issue is filed**
  - SECURITY issues are automatically embargoed.
  - Issues in other projects with the “security” label are not automatically embargoed.
- **Triage** – Happens in-between our weekly meetings.
- **Issue creation**
  - SECURITY issue (if there is one) contains full details and remains embargoed.
    - These follow the Security Team workflow. Often there are many issues which are linked to these.
  - Issues are created for dev teams and linked to SECURITY issues. These have only relevant details and can be viewed by the team.
    - These follow the team’s workflow. Security Team does not transition these from one state to another.
- **Backporting and CSP approvals**
  - If cross-cutting (affecting many modules/teams), Security Team will request CSP approval.
  - If specific to one team, the PO will request CSP approval.
- **Review, Closing, and Disclosure**
  - Upon completion, SECURITY issues are unembargoed and marked Completed.
  - Issues which are not applicable to FOLIO are unembargoed and marked Rejected.

Image by Arcady
@ https://stock.adobe.com

# Severe Issues, e.g. Log4Shell

- Responsible Disclosure
- Issue Details and Remediation advice
  - Are you affected?
  - Workarounds/Fixes
- Tracking
  - Sometimes we setup tooling (E.g. GitHub Actions) to help track status of vulnerabilities affecting numerous modules.
- Retrospective / Post-mortem
  - How did we do?  Were there gaps in our processes?  What can we do better next time?

Image by wifesun
@ https://stock.adobe.com

# Responsible Disclosure

From Wikipedia:

*…a vulnerability disclosure model in which a vulnerability or an issue is disclosed to the public only after the responsible parties have been allowed sufficient time to patch or remedy the vulnerability or issue.*

- "Responsible parties" are usually #sys-ops, and the FOLIO Councils.
- Typically measured in days/weeks

Image by pngtree.com

# False Alarms

Many vulnerabilities reported don't affect FOLIO...

- Closed as "Won't Do" and unembargoed (SECURITY project)
- Semi-automatic process to "ignore" these vulnerabilities in various tools (Snyk/Semgrep/etc)
- Duplicates are unfortunate, but unavoidable
- Significant overhead
- Sometimes requires ongoing monitoring

# How can we improve FOLIO security?

- **Adopt secure coding standards** – Ideally secure coding practices are part of developer onboarding for all teams/devs.
- **Review anything AI generated** – AI tools like Co-pilot can provide a productivity boost, by can also inadvertently introduce security issues.
- **Identify security champions** – Experienced developers who are willing and able to learn more about secure coding practices and serve as advocates in the FOLIO development community.
- **Get more organized!** – With so many ways vulnerabilities are identified/reported, it can be difficult to stay on top of what's what. Consolidating vulnerability data and creating dashboards can be a big help.
- **Ask for our input** – Please feel free to reach out for out input on any security-related matters. We don't bite, I promise!
- **Other ideas?** – We'd love to hear your ideas for improving Folio security.

# Careful with AI-Generated Code!

*“Artificial intelligence models have become increasingly adept at generating computer code. They are powerful and promising tools for software development across many industries, but they can also pose direct and indirect cybersecurity risks.”*

https://cset.georgetown.edu/publication/cybersecurity-risks-of-ai-generated-code/

*“Veracode has unveiled its 2025 GenAI Code Security Report, revealing critical security flaws in AI-generated code. The study analysed 80 curated coding tasks across more than 100 large language models (LLMs), revealing that while AI produces functional code, it introduces security vulnerabilities in 45 per cent of cases.”*

https://www.eenewseurope.com/en/report-finds-ai-generated-code-poses-security-risks/

# Vulnerability Consolidation and Dashboarding Initiative

Snyk provides a dashboard, but is quite limited, especially for a project of FOLIO's size w/ many repositories…

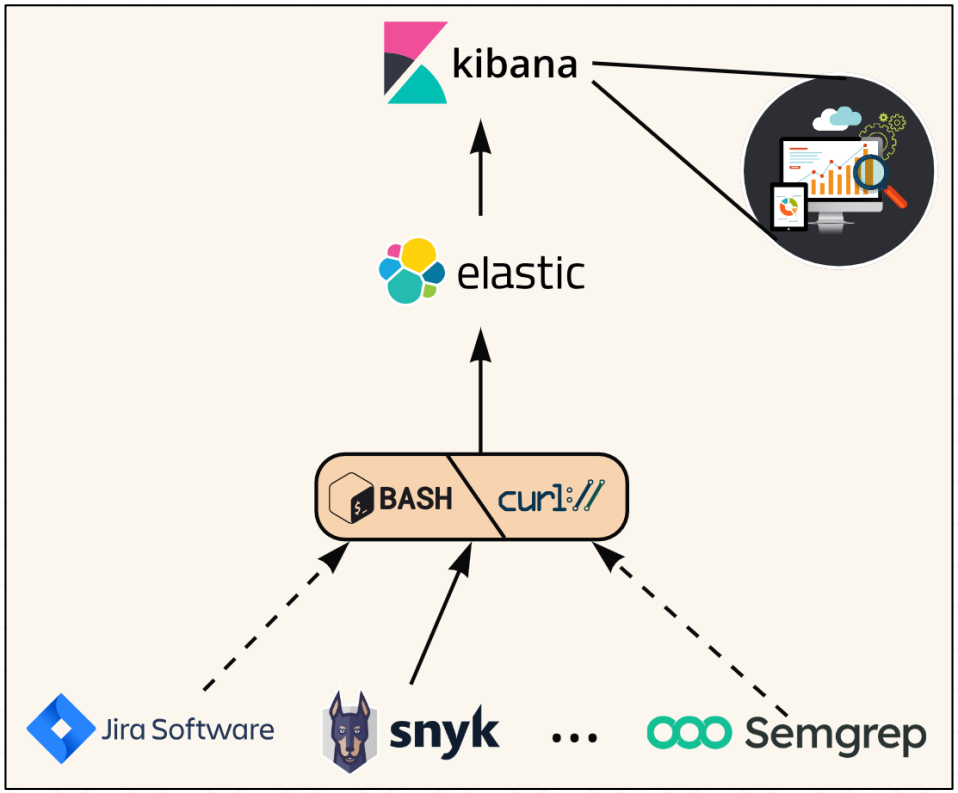
- Scripts to pull data from Snyk into Elasticsearch w/ Kibana dashboards (locally, run daily)
- Greater visibility / continuous monitoring
  - Ability to filter and drill down (e.g. filter out testing repos, or see metrics for only certain components)
  - Identify hot spots (components with many vulnerabilities)
  - Does a vulnerabilities affect many components or few?
  - Spot trends
- Improved querying and tracking
  - Time series data… reported vs fixed
  - Easy to see newly found vulnerabilities


Image by Delices_89
@ freeimages.com

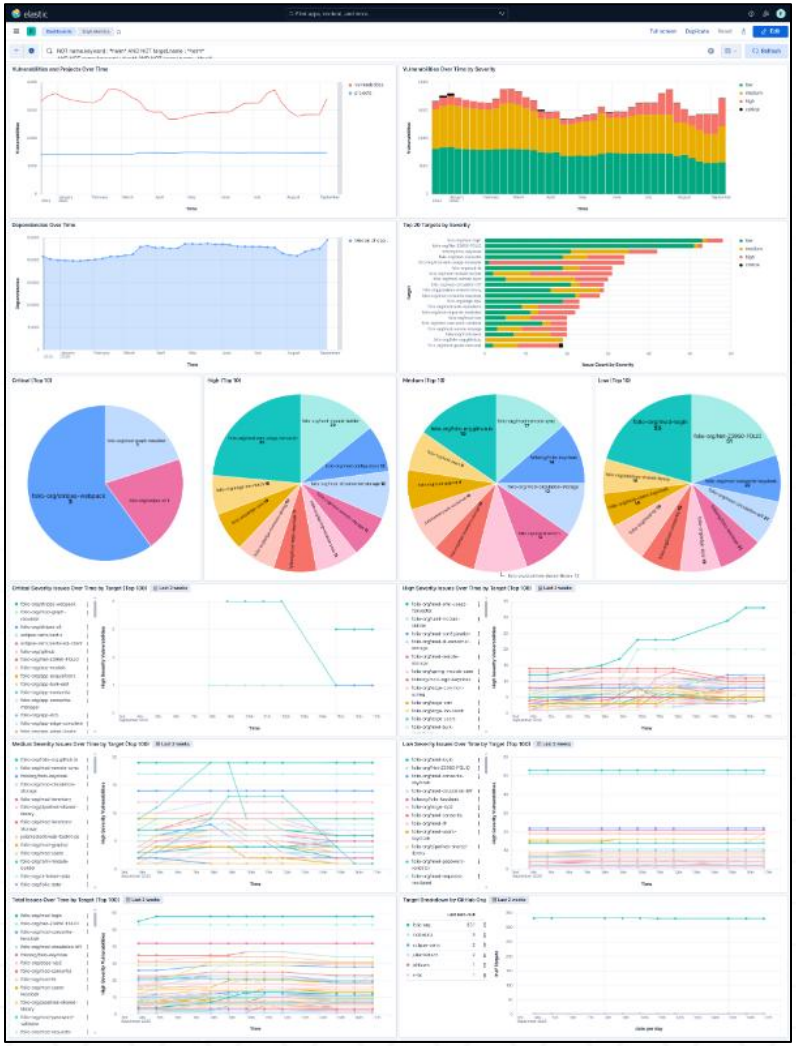
# Vulnerability Consolidation and Dashboarding Initiative - Continued

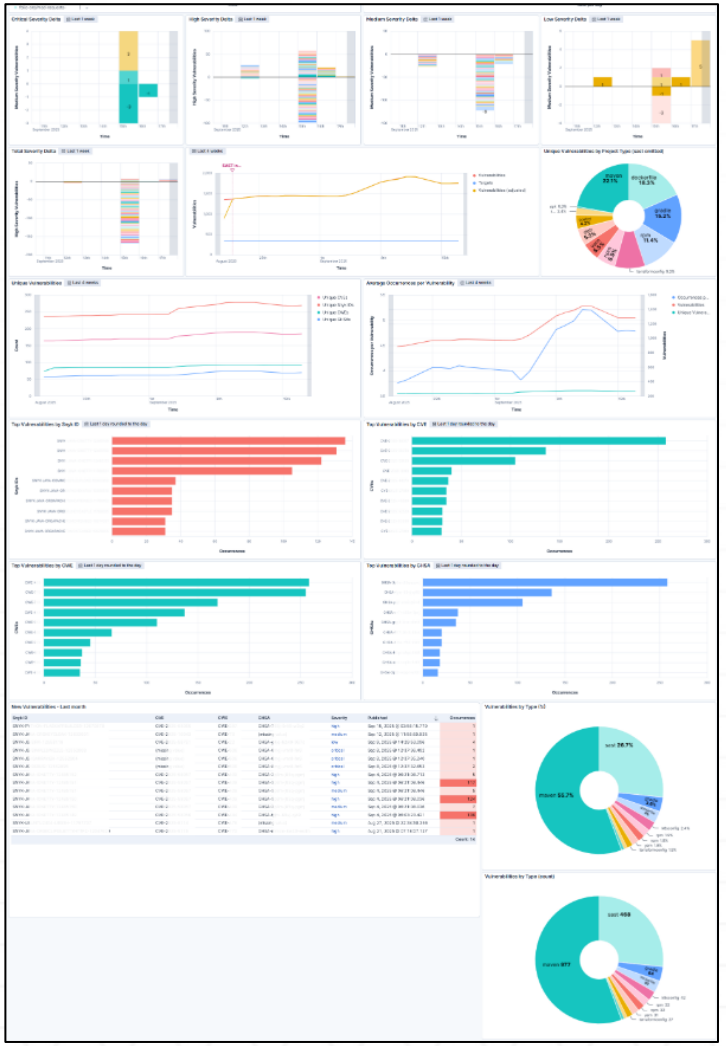
Next Steps:

- Extend to pull data from other sources:
  - Semgrep – Documented APIs!
  - JIRA?
  - Others?
- Formalize and make available to other Security Team members



# Vulnerability Consolidation and Dashboarding Initiative - Continued

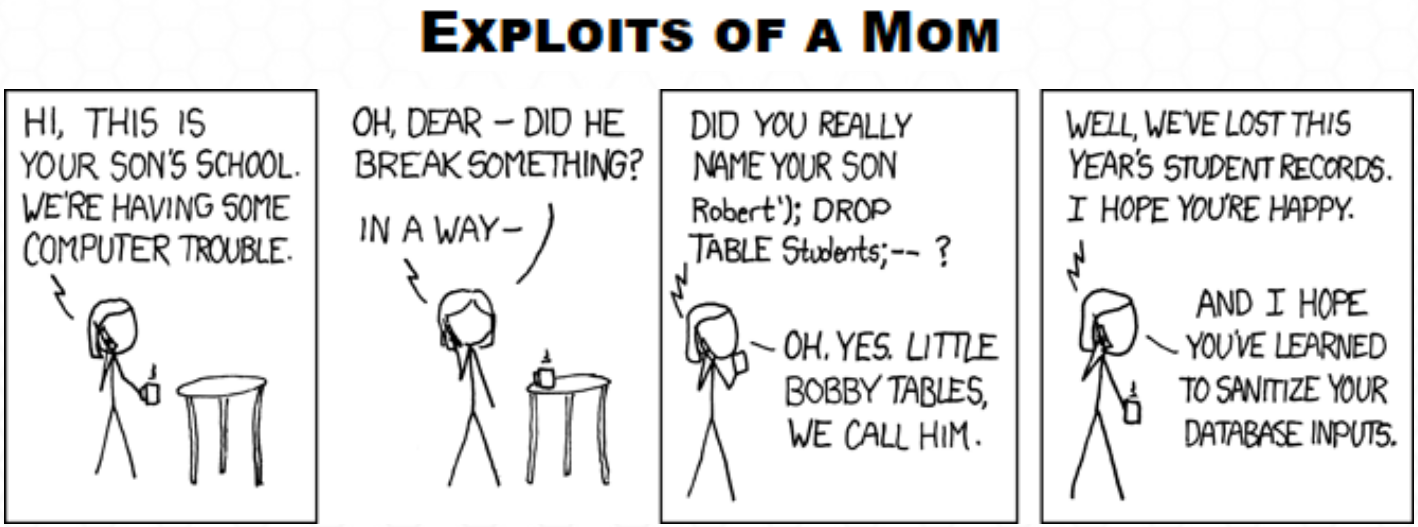




# Additional Information

- FOLIO Vulnerability and Remediation Policy
- Security Team Charter
- Safe Harbor Statement
- Deprecation Policy for unsupported Folio modules with Severe Security Vulnerabilities

# Questions?




https://xkcd.com/327

# FOLIO

*The Future of Libraries is Open*

# THANK YOU

**Craig McNally** | Folio Security Team

@FOLIO_LSP

cmcnally@ebsco.com