MDTP

# How HMRC Digital secures services at scale

**Ben Conrad, HMRC**
**Gerald Benischke, Equal Experts**

HM Revenue
& Customs

EQUAL
EXPERTS

# Multi-channel Digital Tax Platform: Simple, Secure Services For All

MDTP

HM Revenue
& Customs

| | Simple | Secure Services | for All |
|---|---|---|---|
| Users | Consistent and Intuitive | Safe | Accessible and Guided |
| Service Teams | Paved Road | AppSec supported | People Centred |
| Platform Teams | Opinionated Tech Stack | No Humans Allowed | Mixed Suppliers |

The Paved Road is …

A concept, formalizing a set of expectations and commitments between the centralized teams and our engineering customers

Slide borrowed from Netflix

# Find, Fix and Preferably Prevent Security Issues in Applications

# Risks to Services

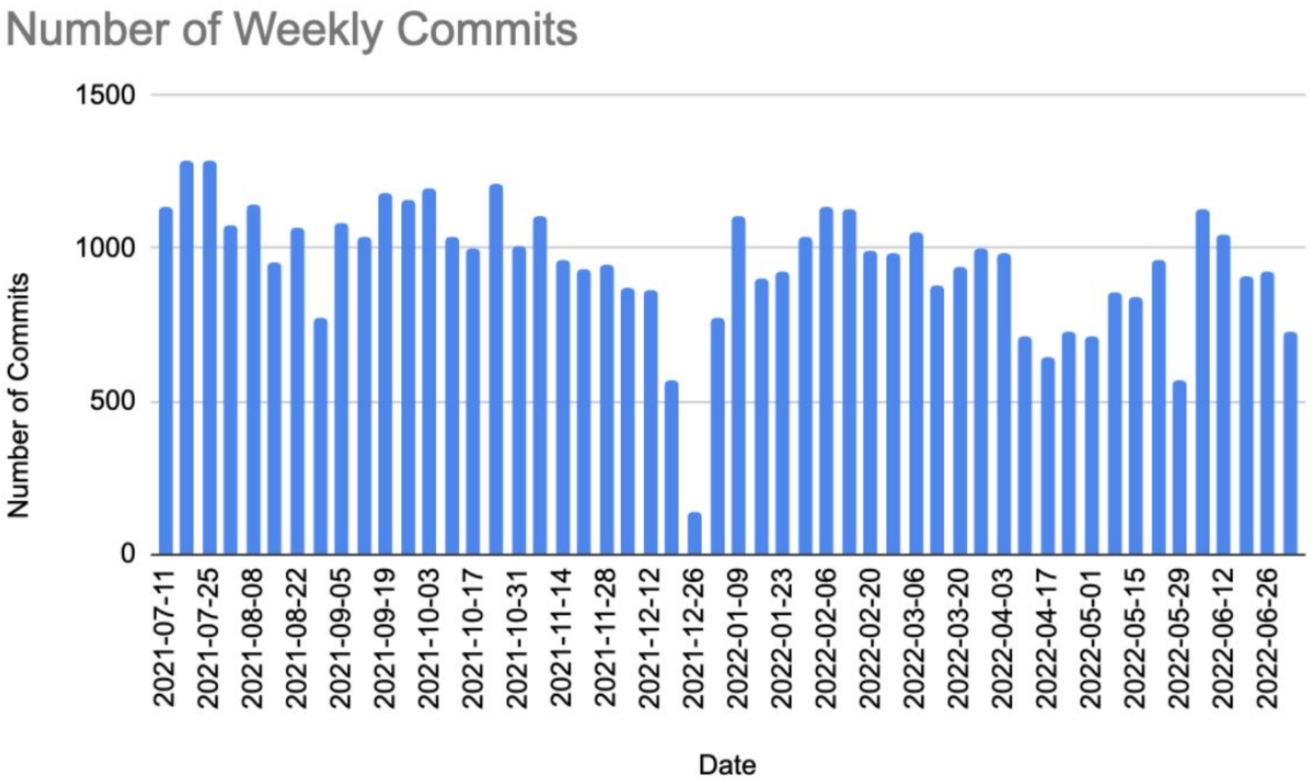
- Rogue engineers
- Script kiddies
- Fraudsters
- Hackers
- Nation States

Last 12 months:

Number of lines changed:
36,000,000

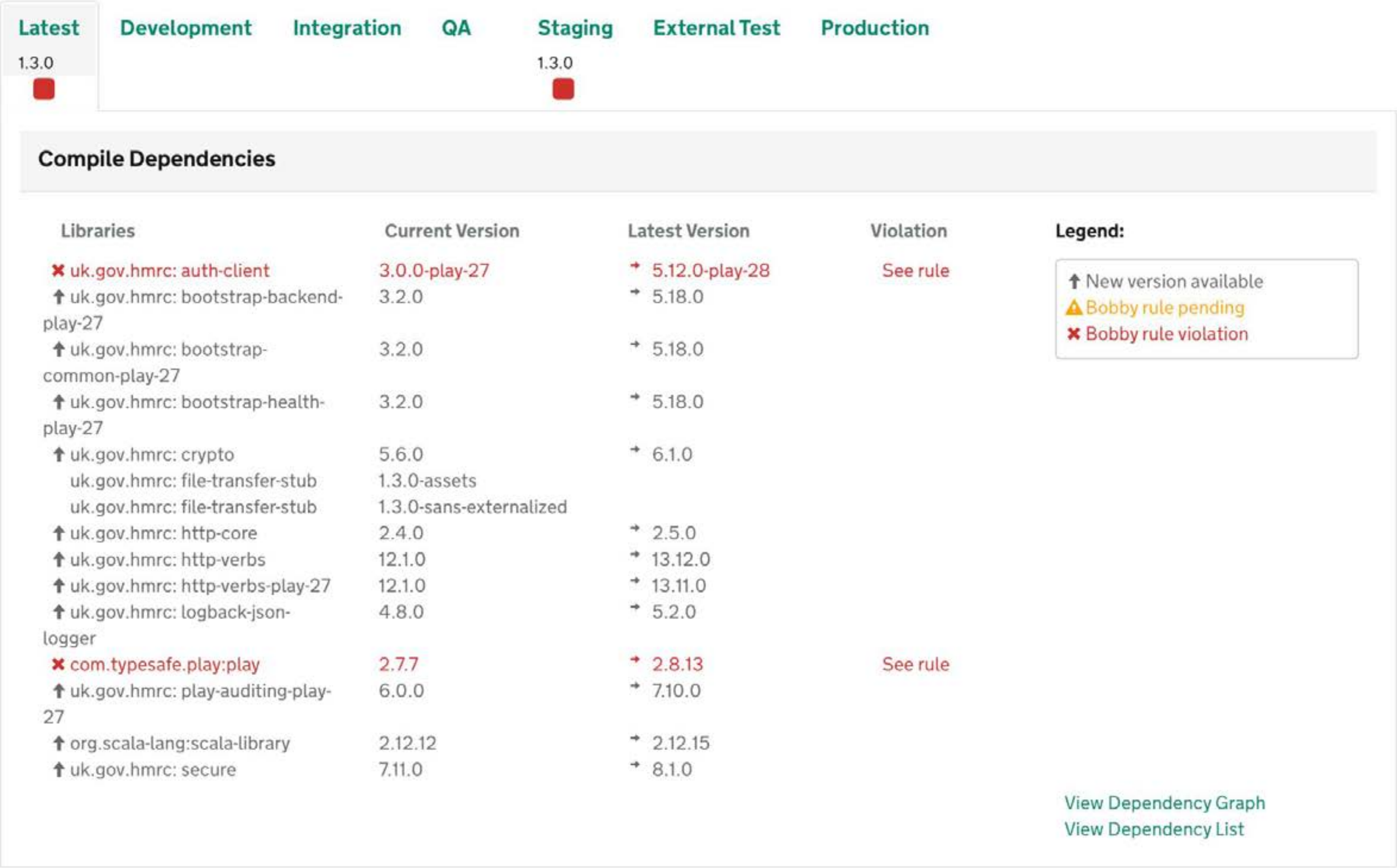
Authors:
640

Repositories:
1187



# Git Commits - Services

# How Do We Do AppSec?



| Latest | Development | Integration | QA | Staging | External Test | Production |
|---|---|---|---|---|---|---|
| 1.3.0<br>🟥 | | | | 1.3.0<br>🟥 | | |

### Compile Dependencies

| Libraries | Current Version | Latest Version | Violation |
|---|---|---|---|
| ✖ uk.gov.hmrc: auth-client | 3.0.0-play-27 | → 5.12.0-play-28 | See rule |
| ↑ uk.gov.hmrc: bootstrap-backend-play-27 | 3.2.0 | → 5.18.0 | |
| ↑ uk.gov.hmrc: bootstrap-common-play-27 | 3.2.0 | → 5.18.0 | |
| ↑ uk.gov.hmrc: bootstrap-health-play-27 | 3.2.0 | → 5.18.0 | |
| ↑ uk.gov.hmrc: crypto | 5.6.0 | → 6.1.0 | |
| uk.gov.hmrc: file-transfer-stub | 1.3.0-assets | | |
| uk.gov.hmrc: file-transfer-stub | 1.3.0-sans-externalized | | |
| ↑ uk.gov.hmrc: http-core | 2.4.0 | → 2.5.0 | |
| ↑ uk.gov.hmrc: http-verbs | 12.1.0 | → 13.12.0 | |
| ↑ uk.gov.hmrc: http-verbs-play-27 | 12.1.0 | → 13.11.0 | |
| ↑ uk.gov.hmrc: logback-json-logger | 4.8.0 | → 5.2.0 | |
| ✖ com.typesafe.play:play | 2.7.7 | → 2.8.13 | See rule |
| ↑ uk.gov.hmrc: play-auditing-play-27 | 6.0.0 | → 7.10.0 | |
| ↑ org.scala-lang:scala-library | 2.12.12 | → 2.12.15 | |
| ↑ uk.gov.hmrc: secure | 7.11.0 | → 8.1.0 | |

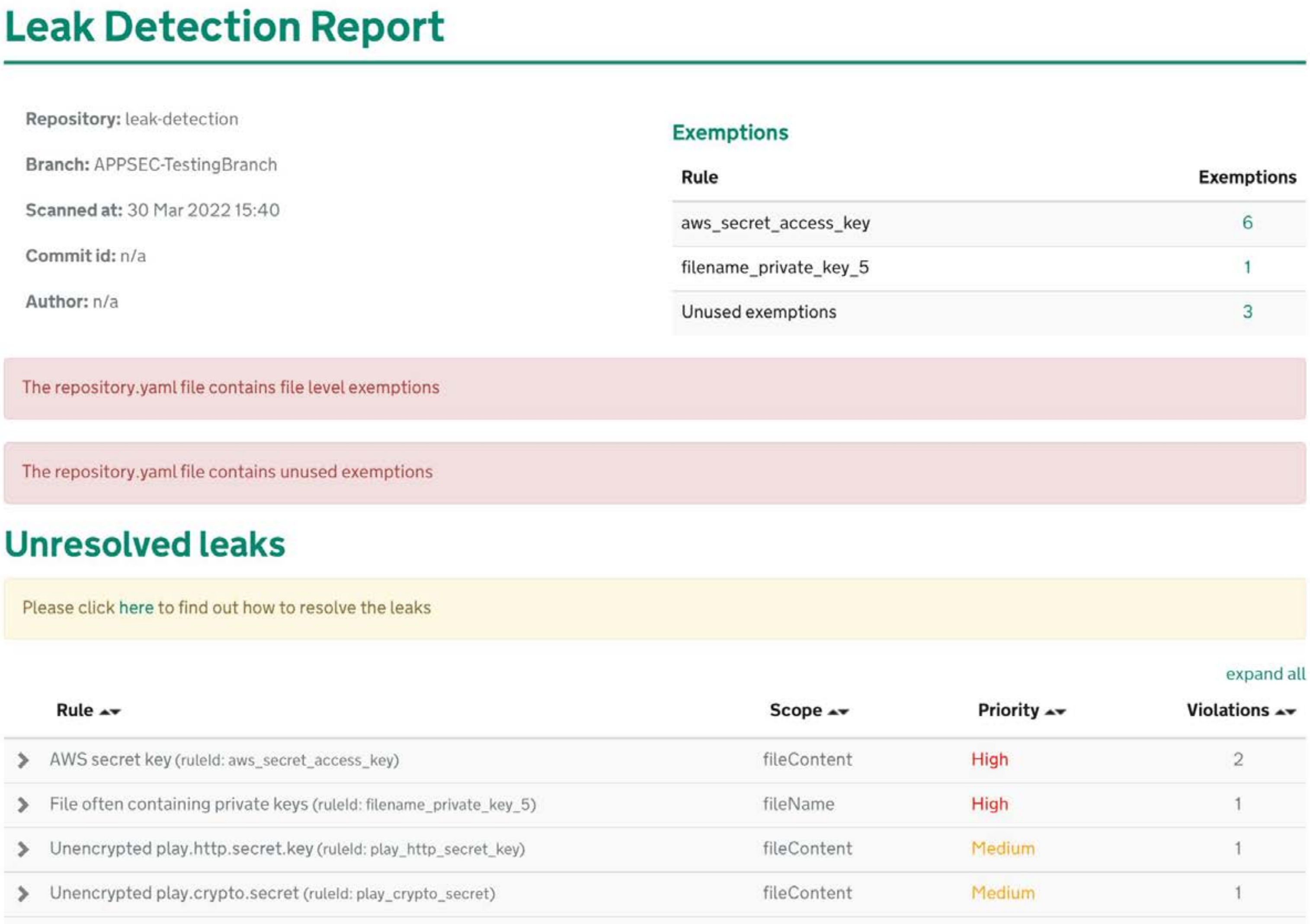
**Legend:**

↑ New version available
⚠ Bobby rule pending
✖ Bobby rule violation

View Dependency Graph
View Dependency List

## Bobby Rules stop dependencies from being used in builds

# Leak Detection



## Leak Detection Report

**Repository:** leak-detection

**Branch:** APPSEC-TestingBranch

**Scanned at:** 30 Mar 2022 15:40

**Commit id:** n/a

**Author:** n/a

### Exemptions

| Rule | Exemptions |
|---|---|
| aws_secret_access_key | 6 |
| filename_private_key_5 | 1 |
| Unused exemptions | 3 |

The repository.yaml file contains file level exemptions

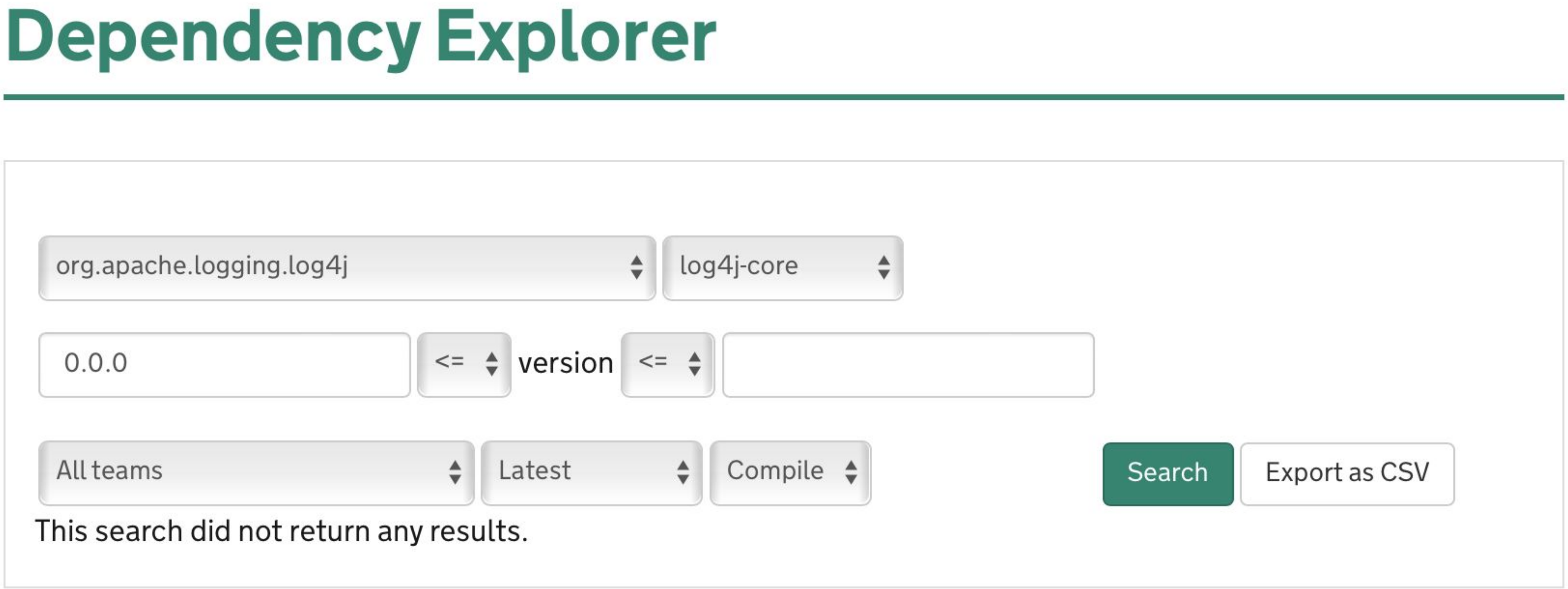
The repository.yaml file contains unused exemptions

## Unresolved leaks

Please click here to find out how to resolve the leaks

expand all

| Rule ▴▾ | Scope ▴▾ | Priority ▴▾ | Violations ▴▾ |
|---|---|---|---|
| AWS secret key (ruleId: aws_secret_access_key) | fileContent | High | 2 |
| File often containing private keys (ruleId: filename_private_key_5) | fileName | High | 1 |
| Unencrypted play.http.secret.key (ruleId: play_http_secret_key) | fileContent | Medium | 1 |
| Unencrypted play.crypto.secret (ruleId: play_crypto_secret) | fileContent | Medium | 1 |



Dependency Explorer

org.apache.logging.log4j

log4j-core

0.0.0 <= version <=

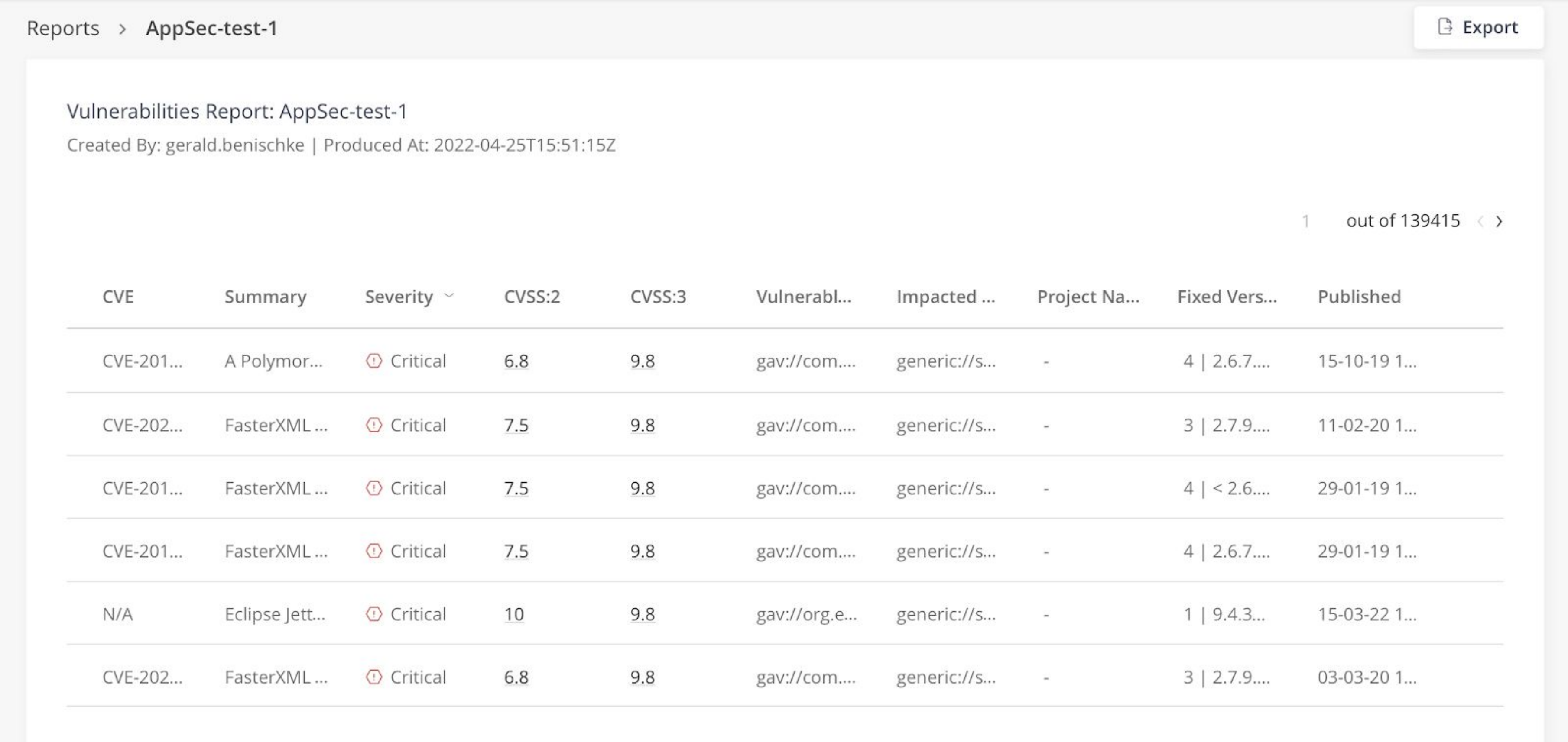
All teams

Latest

Compile

This search did not return any results.

# Catalogue - Dependency Explorer



Vulnerabilities Report: AppSec-test-1

Created By: gerald.benischke | Produced At: 2022-04-25T15:51:15Z

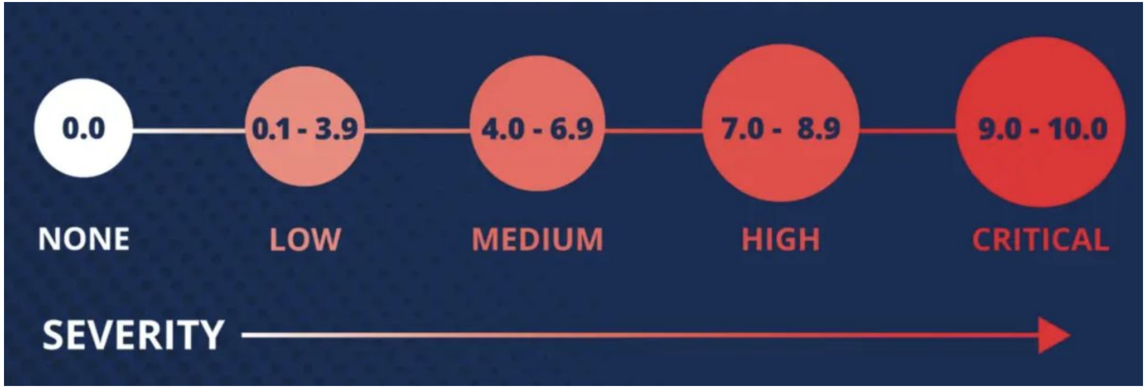
1 out of 139415

| CVE | Summary | Severity | CVSS:2 | CVSS:3 | Vulnerabl... | Impacted ... | Project Na... | Fixed Vers... | Published |
|---|---|---|---|---|---|---|---|---|---|
| CVE-201... | A Polymor... | Critical | 6.8 | 9.8 | gav://com.... | generic://s... | - | 4 \| 2.6.7.... | 15-10-19 1... |
| CVE-202... | FasterXML ... | Critical | 7.5 | 9.8 | gav://com.... | generic://s... | - | 3 \| 2.7.9.... | 11-02-20 1... |
| CVE-201... | FasterXML ... | Critical | 7.5 | 9.8 | gav://com.... | generic://s... | - | 4 \| < 2.6.... | 29-01-19 1... |
| CVE-201... | FasterXML ... | Critical | 7.5 | 9.8 | gav://com.... | generic://s... | - | 4 \| 2.6.7.... | 29-01-19 1... |
| N/A | Eclipse Jett... | Critical | 10 | 9.8 | gav://org.e... | generic://s... | - | 1 \| 9.4.3... | 15-03-22 1... |
| CVE-202... | FasterXML ... | Critical | 6.8 | 9.8 | gav://com.... | generic://s... | - | 3 \| 2.7.9.... | 03-03-20 1... |

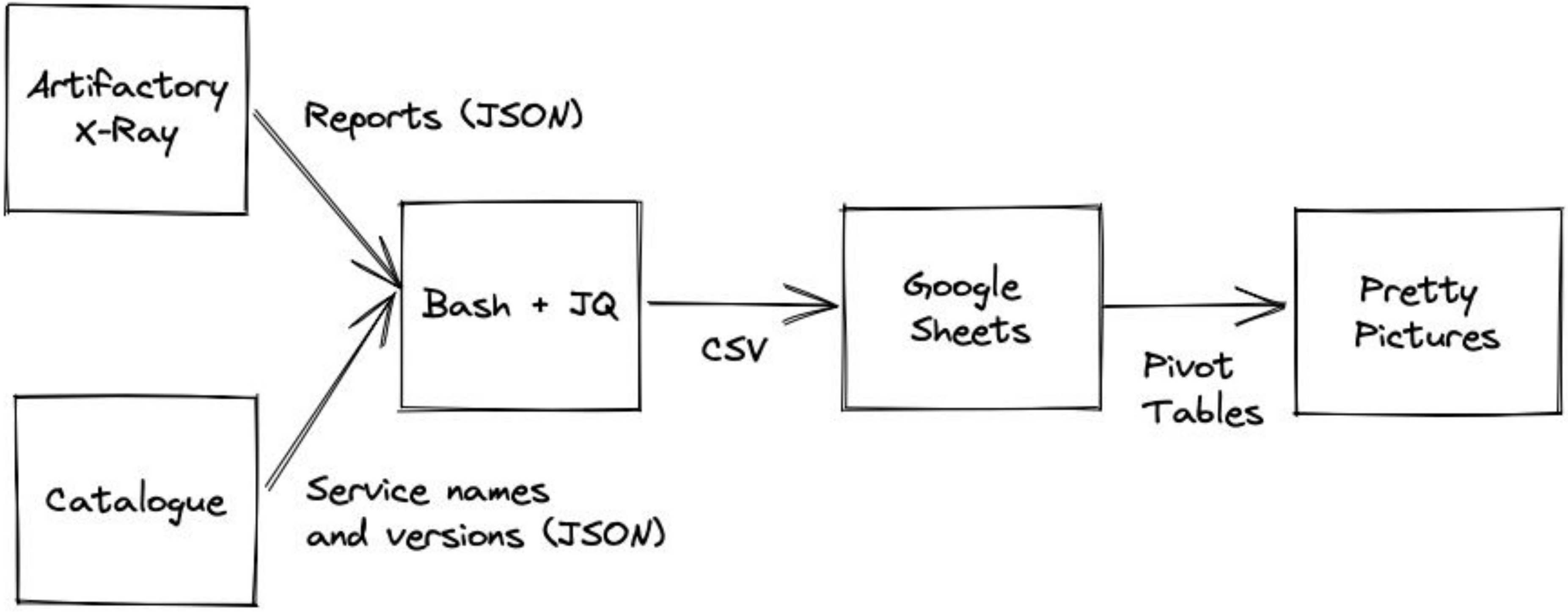
X-Ray reports not very user friendly

# CVSS Scores Not That Useful

- Investigated each CVE
- CVSS Score is NOT a predictor of risk
- Most frequent root cause is not an issue on the platform
- It does not work this way:

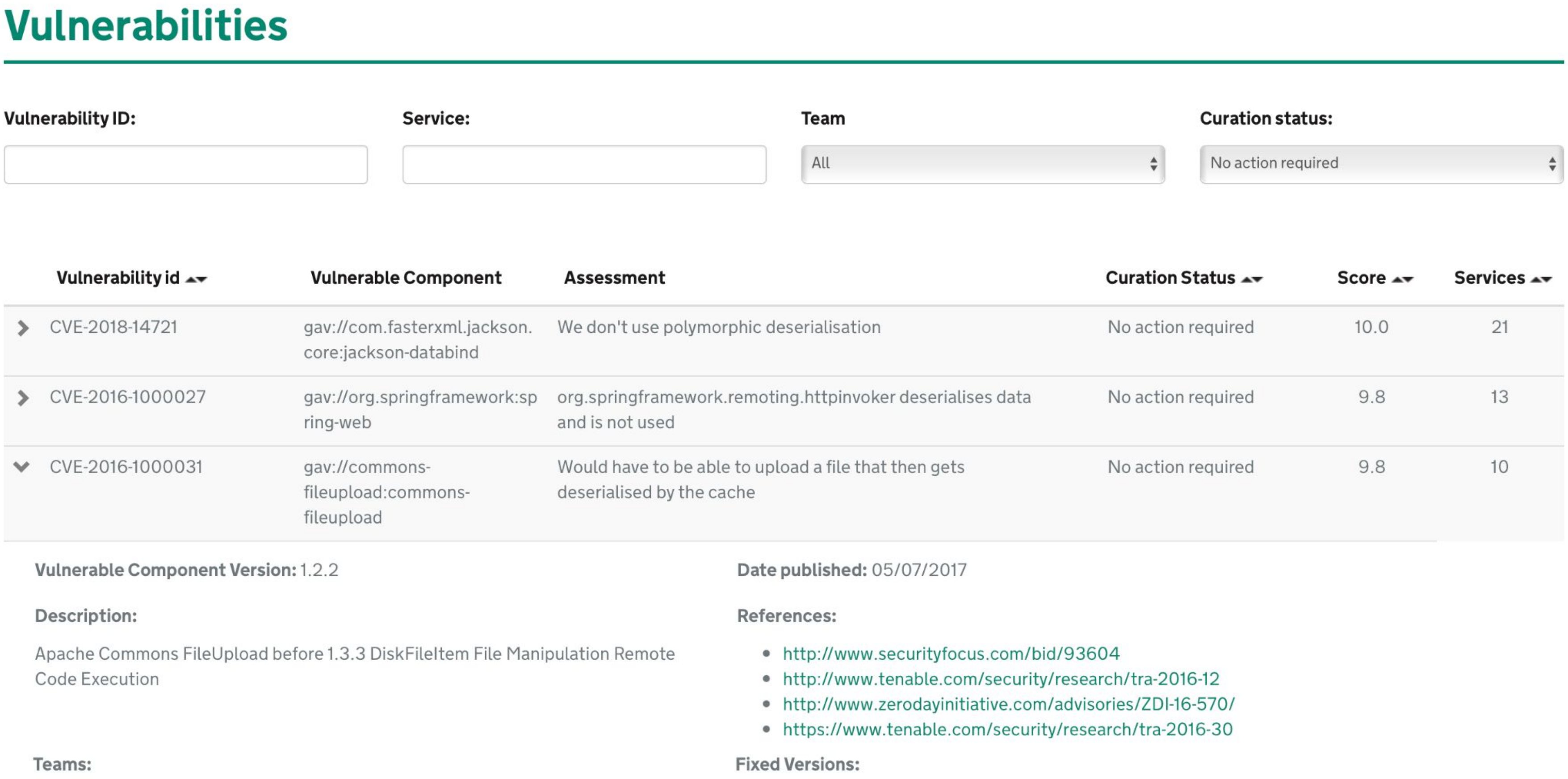


# Evaluate Dependencies - Spreadsheets to the Rescue



# Vulnerabilities Tooling

| | As a Service Engineer | As an AppSec Engineer | As a Risk Owner |
|---|---|---|---|
| MVP | See CVEs<br>View Only Actions<br>Details<br>Team Summary | Metrics<br>Manual Upload<br>Spread sheets | High Level Summary |
| Iteration 1 | | Automatic Upload<br>Prioritise | |
| Iteration 2 | Team Trends<br>Self Serve Curation | CVE Trends<br>Monitor Actions | High Level Trends<br>Overall Health |



# Vulnerabilities

Vulnerability ID:

Service:

Team: All

Curation status: No action required

| Vulnerability id | Vulnerable Component | Assessment | Curation Status | Score | Services |
|---|---|---|---|---|---|
| CVE-2018-14721 | gav://com.fasterxml.jackson.core:jackson-databind | We don't use polymorphic deserialisation | No action required | 10.0 | 21 |
| CVE-2016-1000027 | gav://org.springframework:spring-web | org.springframework.remoting.httpinvoker deserialises data and is not used | No action required | 9.8 | 13 |
| CVE-2016-1000031 | gav://commons-fileupload:commons-fileupload | Would have to be able to upload a file that then gets deserialised by the cache | No action required | 9.8 | 10 |

**Vulnerable Component Version:** 1.2.2

**Date published:** 05/07/2017

**Description:**

Apache Commons FileUpload before 1.3.3 DiskFileItem File Manipulation Remote Code Execution

**References:**

- http://www.securityfocus.com/bid/93604
- http://www.tenable.com/security/research/tra-2016-12
- http://www.zerodayinitiative.com/advisories/ZDI-16-570/
- https://www.tenable.com/security/research/tra-2016-30

**Teams:**

**Fixed Versions:**

Catalogue Vulnerabilities

# Risk Ledger

- Which services are frontend/backend/admin?
- What are all the endpoints from all services?
- Which services store data?
- Which services parse files?
- Which services generate files?
- Which services access third-party services?
- Which services process XML?

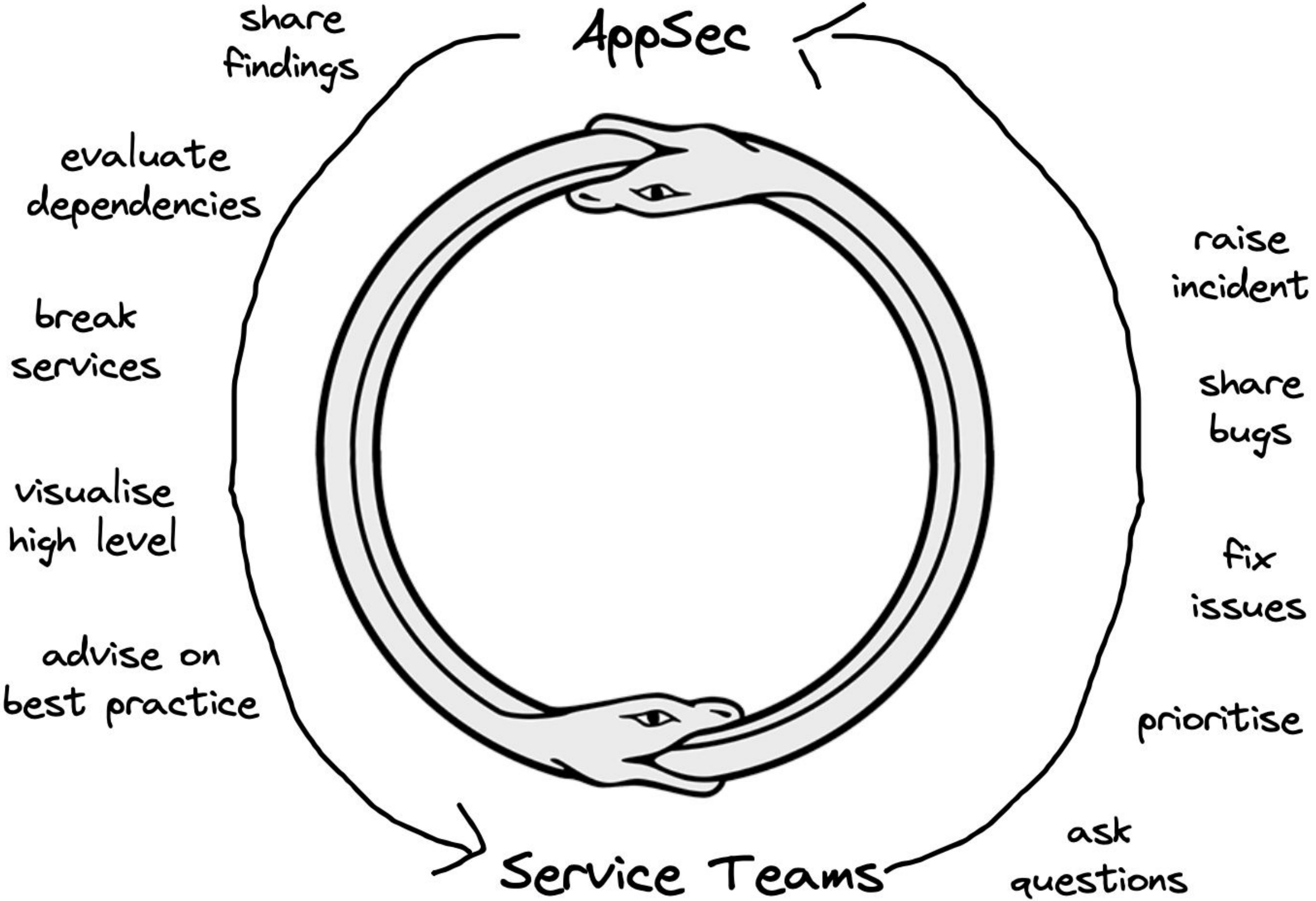
# Where Do Security Specialists Sit?

In the service team (decentralised):

- Do we really have the £££ for 100 security experts?
- Won’t they just spend most of their time analysing the same issues?
- Will deadlines and project work allow time to go back to fix issues?

In a Security team (centralised):

- Won’t they just be a bottleneck if 100 teams need help at the same time?
- Can’t investigate everything
- Don’t understand the context of service code



AppSec

share findings

evaluate dependencies

break services

visualise high level

advise on best practice

Service Teams

ask questions

prioritise

fix issues

share bugs

raise incident

# MDTP Opinions Enable AppSec

# Conclusions

- Paved Road helps
- Tooling helps
- Experienced Engineers

# Thank you!

Ben Conrad, Head of Product, HMRC
Gerald Benischke, AppSec Snooper, Equal Experts, @beny23@infosec.exchange

42

HM Revenue
& Customs

MDTP

EQUAL
EXPERTS