NDSU | COMPUTER SCIENCE

Capstone 2024

OpenStack Manila – Bandit Integration

Team Members: Annwesha Das, Elvis Acheampong, Skylar Markegard

Sponsor: OpenStack

Project Plans

- Integrate Bandit into OpenStack Manila's tox environment to scan their code repositories for security issues
- Integrate Bandit's tox environment into Manila's Zuul Continuous Integration for these code repositories
- Fix as many security issues Bandit reports in Manila's code repositories as possible within the timeframe of the project

Project Parts

OpenStack

- Open Source cloud computing platform
- Multiple services offered including networking, cloud computing, and block, object and shared file storage

OpenStack Manila

- OpenStack's shared file storage service
- Extensibility for multiple backends to support vendor and file system specific nuances

Bandit

- Python tool to statically analyze code for security issues
- Uses ASTs and runs plugins against it to make a report

Tox

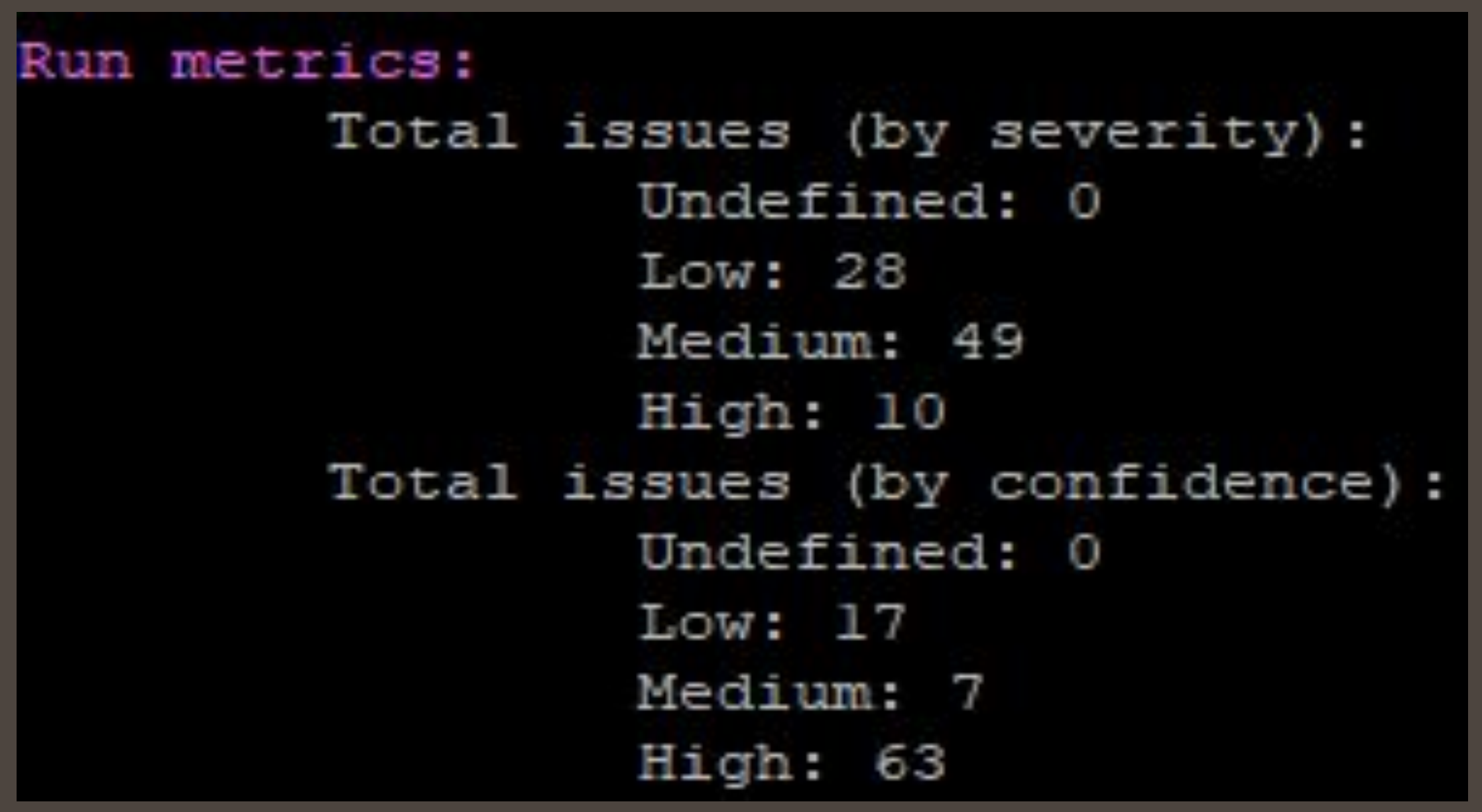
- Virtual environment management and test tool
- Allows running of Bandit tests within its own environment

Zuul

- Continuous integration tool that determines whether a commit is ready to enter a code repository based on tests it is given to run
- Can run the Bandit tox environment on new commits

Development Phase 1

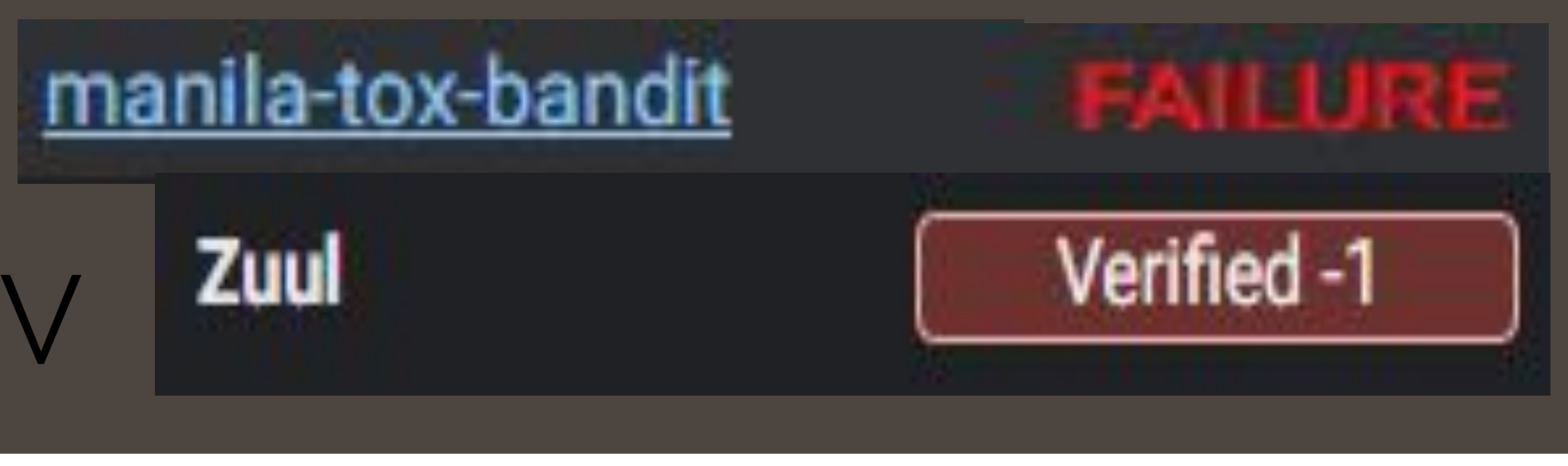
- Successful implementation of Bandit in Tox
- Catalog made of existing security issues



```
Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 28
                Medium: 49
                High: 10
        Total issues (by confidence):
                Undefined: 0
                Low: 17
                Medium: 7
                High: 63
```

- Successful integration of Bandit into Zuul CI flow
- Results of Zuul test visible on OpenDev, OpenStack's code review and project hosting site

opendev

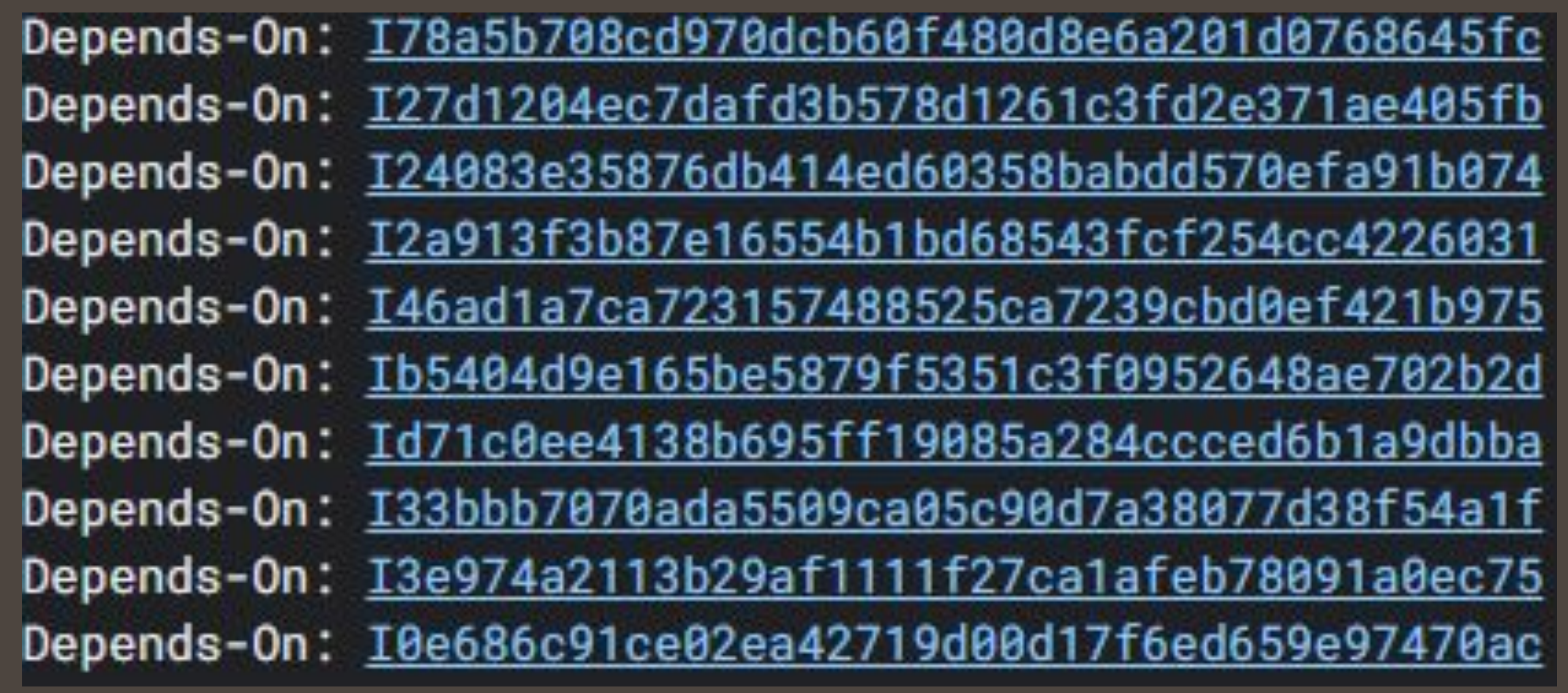


manila-tox-bandit FAILURE

Zuul Verified -1

Development Phase 2

- Beginning squashing of security issues



```
Depends-On: I78a5b708cd970dcb60f480d8e6a201d0768645fc
Depends-On: I27d1204ec7dafd3b578d1261c3fd2e371ae405fb
Depends-On: I24083e35876db414ed60358babdd570efa91b074
Depends-On: I2a913f3b87e16554b1bd68543fcf254cc4226031
Depends-On: I46ad1a7ca723157488525ca7239cbd0ef421b975
Depends-On: Ib5404d9e165be5879f5351c3f0952648ae702b2d
Depends-On: Id71c0ee4138b695ff19085a284ccced6b1a9dbba
Depends-On: I33bbb7070ada5509ca05c90d7a38077d38f54a1f
Depends-On: I3e974a2113b29af1111f27ca1afeb78091a0ec75
Depends-On: I0e686c91ce02ea42719d00d17f6ed659e97470ac
```

Many choices when deciding on how to resolve

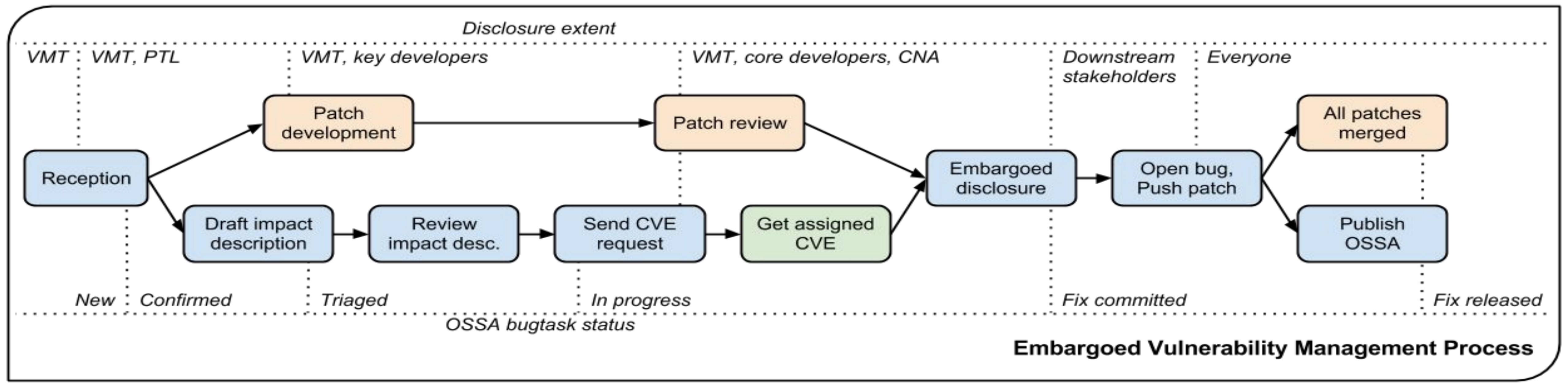
- Is it a false positive?
- What is the intended functionality of the code?
- How would the vulnerability be exploited?

Failing to take these factors into consideration will cause more time to be spent fixing your patch to the issue than the issue itself.

Project Impact

Cybersecurity has become one of the most important aspects of large scale software vendors, such as OpenStack, within recent years. Static code analysis tools are an important part of helping deliver a secure product.

By implementing Bandit into OpenStack Manila's code repositories and continuous integration flow, the project has help harden Manila's cybersecurity. This ensures that Manila stays ahead of any vulnerabilities before they end up introduced into their code and the client can have a secure project as OpenStack goes forward with re-evaluating its Security Management and Vulnerability Management Team processes.



Embargoed Vulnerability Management Process