

ARVOS

AI- and Risk-based Vulnerability
Management
for Trustworthy Open Source Adoption

debricked



Emil Wåreus

**Co-Founder &
Head of Data Science**

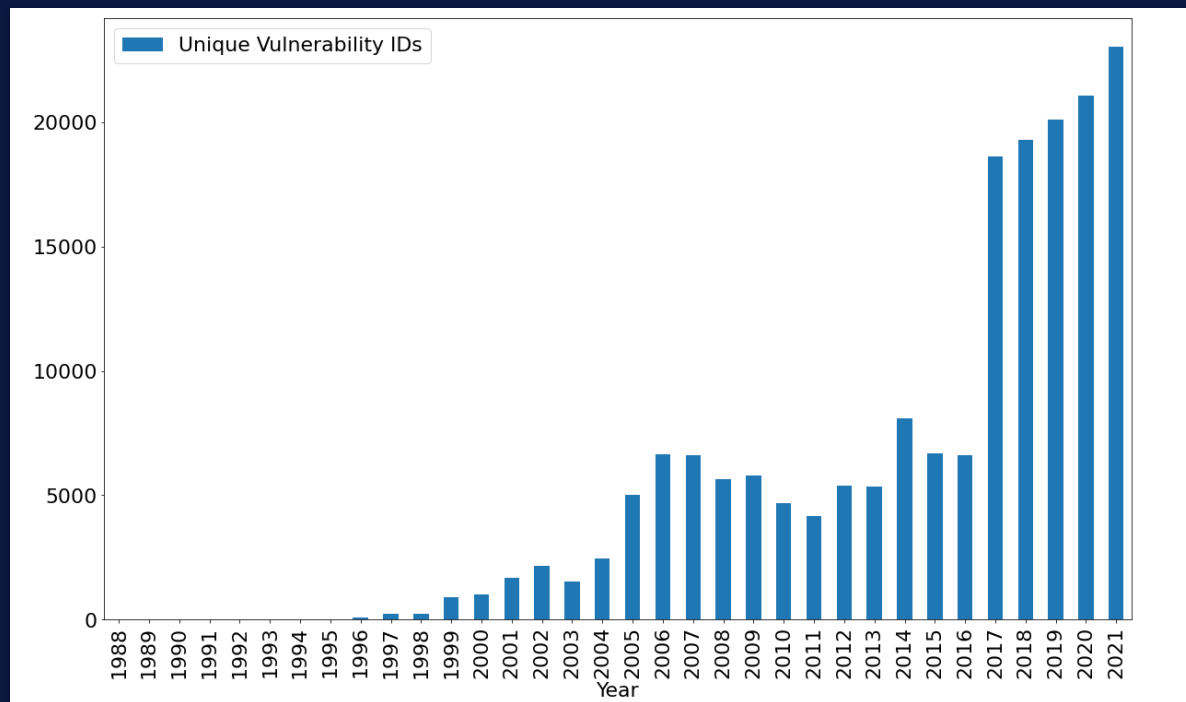
emil.wareus@debricked.com



Vulnerabilities in Open Source

More vulnerabilities
discovered each year

More alerts and work
required for developers



The “Cry Wolf” problem

Large lists of vulnerabilities to handle

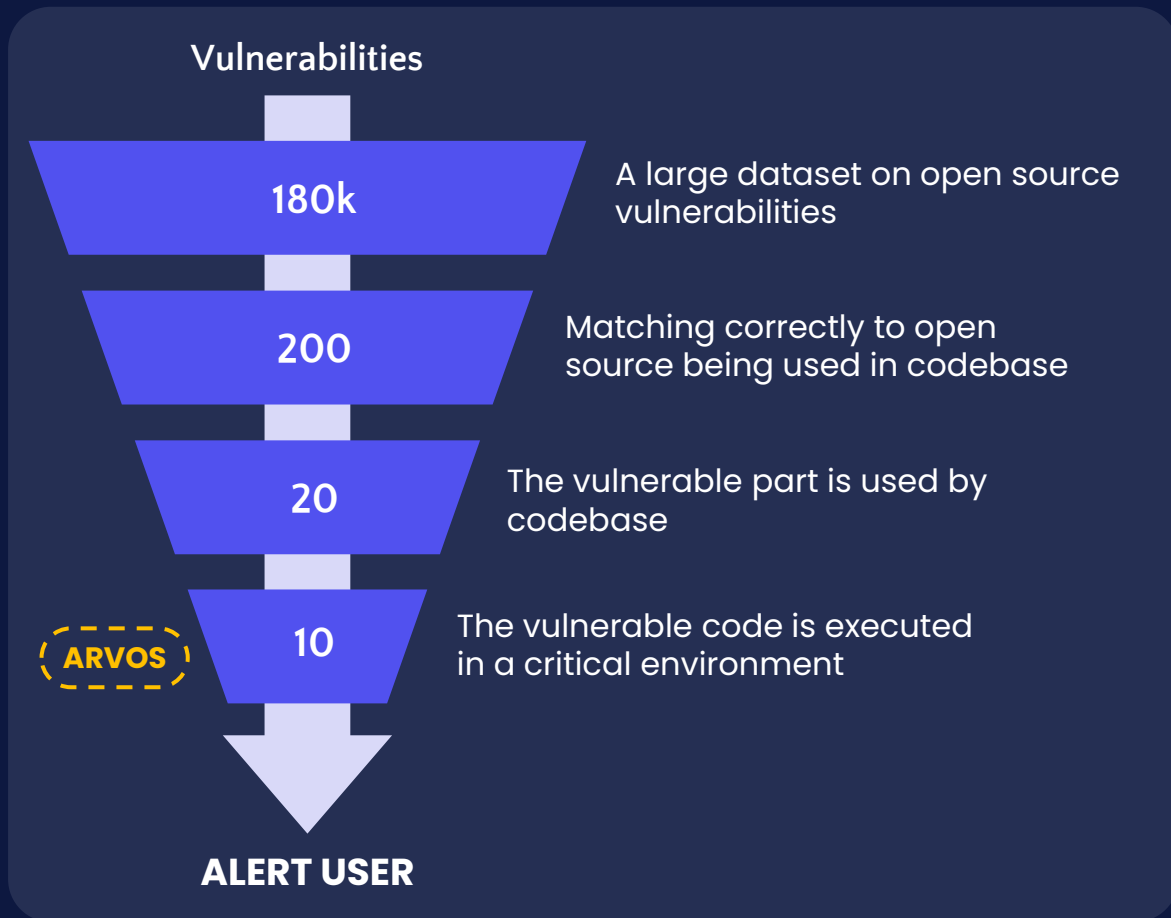
Rich information on the vulnerability itself

Poor contextualization to my code

Vulnerabilities						
All commits						
Dependencies						
Q Search by name or dependency						
Filter 15 entries						
Name	Discovered	CVSS	debAI	Dependencies	Review status	
CVE-2019-10196	2021-07-01	9.8	80	http-p...		Vulnerable
CVE-2019-10747	2021-07-01	9.8	75	set-va...		Vulnerable
CVE-2021-31597	2021-07-01	9.4	72	xmlht...		Unexamined
CVE-2020-15123	2021-07-01	9.3	66	codec...		Vulnerable
CVE-2021-28918	2021-07-01	9.1	63	netm...		Unexamined
CVE-2019-10744	2021-07-01	9.1	69	lodas...		Unexamined
CVE-2020-7597	2021-07-01	8.8	67	codec...		Unexamined
CVE-2020-7660	2021-07-01	8.1	74	serial...		Unexamined
CVE-2020-28469	2021-07-01	7.5	65	glob...		Unexamined
CVE-2021-33623	2021-07-01	7.5	58	trim-n...		Unexamined
CVE-2021-23343	2021-07-01	7.5	58	path...		Unexamined
CVE-2020-36049	2021-07-01	7.5	58	socke...		Unexamined
CVE-2020-36048	2021-07-01	7.5	58	engin...		Unexamined
CVE-2019-10775	2021-07-01	7.5	58	ecstat...		Unexamined
CVE-2019-20149	2021-07-01	7.5	57	kind...		Unexamined

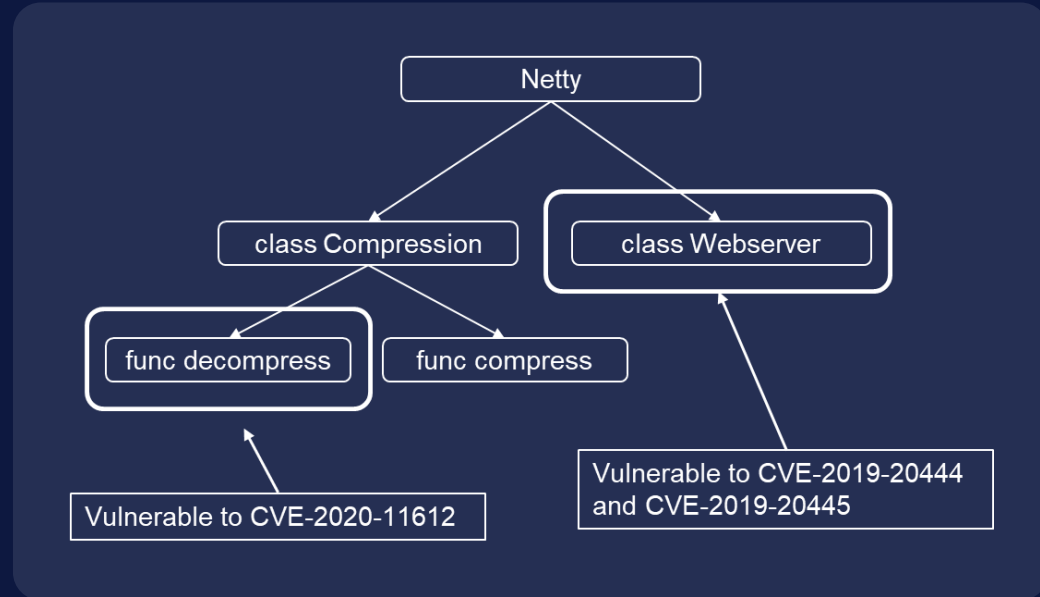
The 4 levels of precision

1. Are you using vulnerable OSS?
2. Are you calling the vulnerable part of the OSS?
3. Is the vulnerable part being called in a critical environment?
4. Is the vulnerability exploitable?

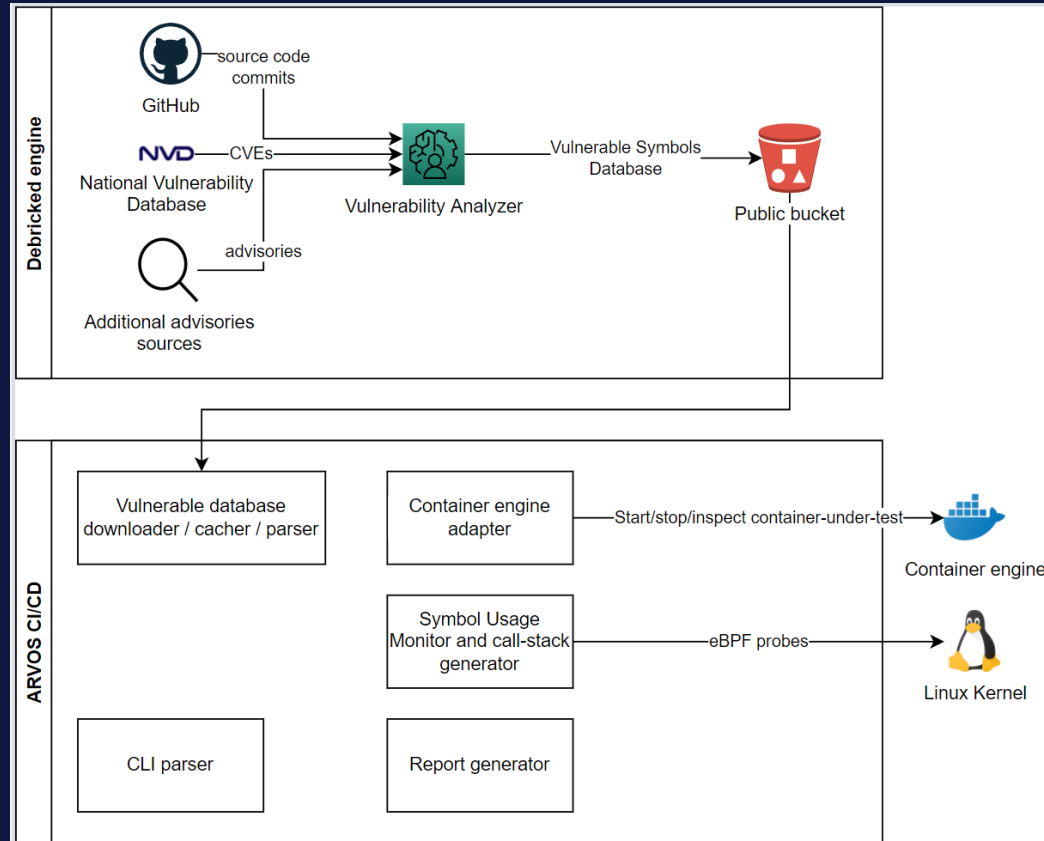


Finding the Vulnerable Functionality

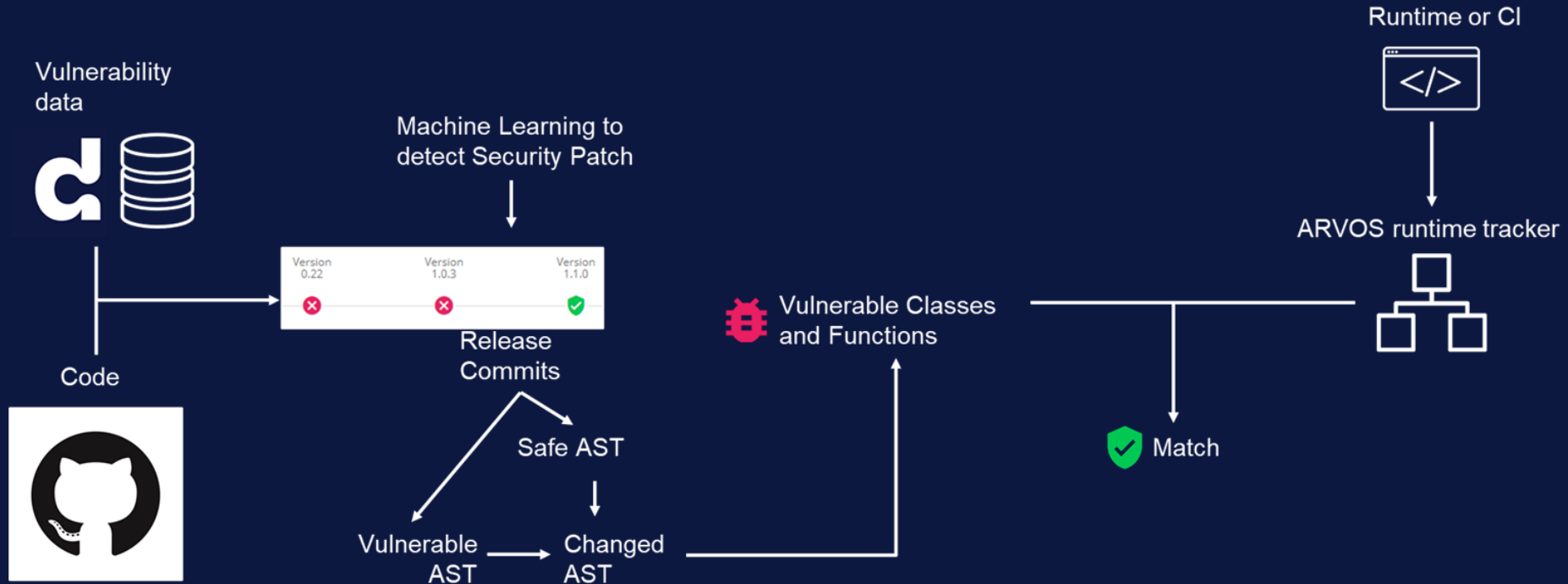
Only a part of the OSS project is affected by the affected vulnerability



ARVOS architecture



Finding the Vulnerable Functionality



Tracing the Vulnerable Function Calls

Trace Vulnerable Code Execution
in your CI

Get stack-trace reports,
displaying how you reached the
vulnerable code

Available as GitHub Action

```
Tracing calls in process 342388 (Language: python)... Ctrl-C to quit.  
^C  
Stopping the tracer .  
Generating Report ...
```

The following vulnerable symbol has been invoked :

```
Vulnerability: CVE-2019-19844  
Vulnerability Detail: https://nvd.nist.gov/vuln/detail/CVE-2019-19844  
Repository: https://github.com/django/django  
Invoked Class: django.forms.widgets.CheckboxInput  
Invoked Method: get_context  
Stacktrace:  
  at /home/elias/.local/lib/python3.10/site-packages/django/forms/widgets.py.get_context:297  
  at /home/elias/.local/lib/python3.10/site-packages/django/forms/widgets.py.get_context:434  
  at /home/elias/.local/lib/python3.10/site-packages/django/forms/widgets.py.render:244  
  at /home/elias/.local/lib/python3.10/site-packages/django/forms/boundfield.py.as_widget:79  
  at /home/elias/.local/lib/python3.10/site-packages/django/utils/html.py.<lambda>:377  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py.render_value_in_context:1011  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py.render_annotated:930  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py.<listcomp>:977  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py.render:976  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py._render:107  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/base.py.render:176  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/backends/django.py.render:58  
  at /home/elias/.local/lib/python3.10/site-packages/django/template/loader.py.render_to_string:52  
  at /home/elias/.local/lib/python3.10/site-packages/django/shortcuts.py.render:14  
  at /home/elias/Documents/arvos/djangoProject/nyapp/views.py.hone:10  
  at /home/elias/.local/lib/python3.10/site-packages/django/urls/resolvers.py.resolve:586  
  at /home/elias/.local/lib/python3.10/site-packages/django/urls/resolvers.py.resolve:586
```

The following vulnerable symbol has been invoked :

```
Vulnerability: CVE-2021-28658  
Vulnerability Detail: https://nvd.nist.gov/vuln/detail/CVE-2021-28658  
Repository: https://github.com/django/django  
Invoked Class: django.http.multipartparser.MultiPartParser  
Invoked Method: parse  
Stacktrace:  
  at /home/elias/.local/lib/python3.10/site-packages/django/http/multipartparser.py.parse:104  
  at /home/elias/.local/lib/python3.10/site-packages/django/http/request.py.parse_file_upload:281  
  at /home/elias/.local/lib/python3.10/site-packages/django/http/request.py.load_post_and_files:312  
  at /home/elias/.local/lib/python3.10/site-packages/django/core/handlers/wsgi.py.get_post:100  
  at /home/elias/Documents/arvos/djangoProject/nyapp/views.py.model_form_upload:13  
  at /home/elias/.local/lib/python3.10/site-packages/django/urls/resolvers.py.resolve:586  
  at /home/elias/.local/lib/python3.10/site-packages/django/urls/resolvers.py.resolve:586  
  at /home/elias/.local/lib/python3.10/site-packages/django/urls/resolvers.py.resolve:586
```

[FAIL] We found 2 vulnerable symbols being used in your application.



Demo

<https://github.com/arvos-dev/spring-vulnerable-app>



Thank you!

emil.wareus@debricked.com

<https://github.com/arvos-dev>