Deep Detection of IaC Security Smells

Ruben Opdebeeck
Ruben.Denzel.Opdebeeck@vub.be
@ROpdebee

Ahmed Zerouali
Ahmed.Zerouali@vub.be
@a_zerou

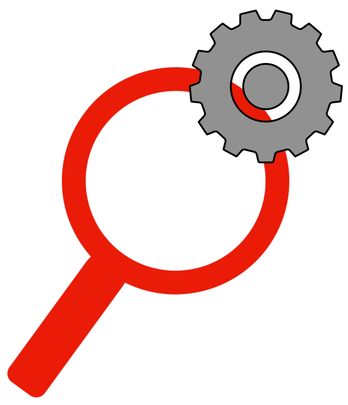
Coen De Roover
Coen.De.Roover@vub.be
@CoenDeRoover

vars.yml
```
# Variables for Ruby installation.
ruby_install_from_source: true
ruby_download_url:
  https://cache.ruby-lang.org/…/ruby-2.7.6.tar.gz
ruby_version: 2.7.6
```

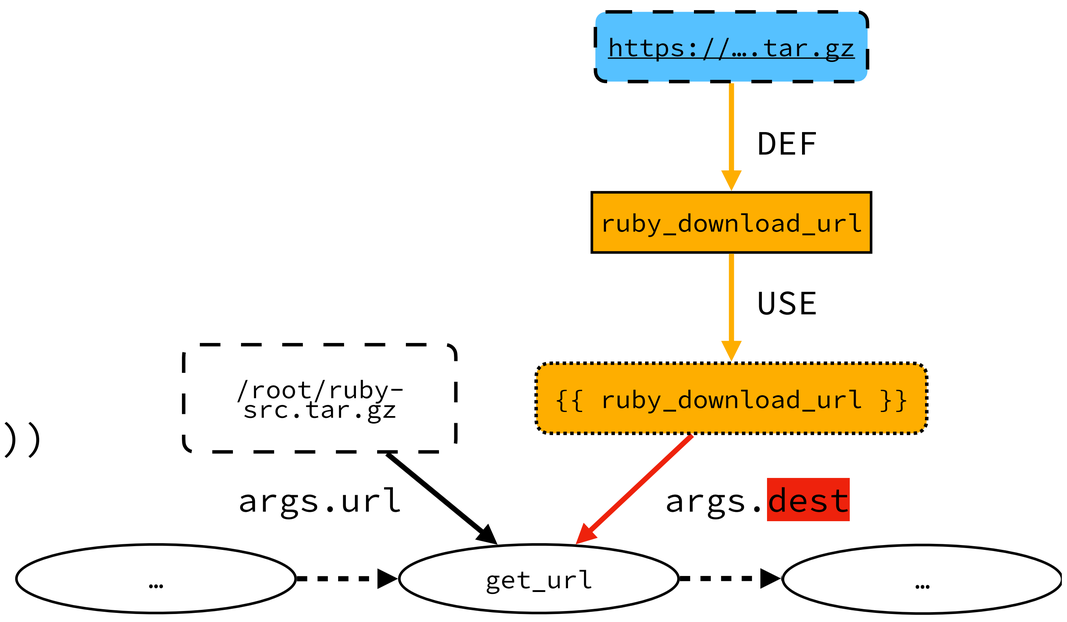
provision.yml
```
- hosts: all
  vars_files: vars.yml
  roles:
    - geerlingguy.ruby
```

geerlingguy/ansible-role-ruby
```
- name: Download ruby.
  get_url:
    url: "{{ ruby_download_url }}"
    dest: "/root/ruby-src.tar.gz"
```

Missing integrity check



```
MATCH chain =
    (source:Literal)
    -[:DEF|USE*0..]->()
    -[arg:KEYWORD]->(sink:Task)
WHERE
    source.value =~ 'http.*.tar.gz'
    AND NOT (()-['checksum']->(sink))
RETURN source;
```



Smell type	# instances	Precision	Recall
Admin By Default	64	98.11%	**81.25%**
Empty Password	15	**44.44%**	**80.00%**
HTTP Without SSL/TLS	35	**100.00%**	**88.57%**
Hardcoded Secret	11	45.45%	**90.91%**
Missing Integrity Check	27	**96.15%**	**92.59%**
Unrestricted IP Address	47	76.60%	76.60%
Weak Crypto Algorithm	44	**97.67%**	**95.45%**

7933 ***unique smells***

472 ***affected repositories***

3613 ***affected files***

33% ***smells cross file boundaries***

55% ***smells involve data flow indirection***

6.5% ***smells involve 3rd party code***

Ruben Opdebeeck, Ahmed Zerouali, Coen De Roover. 2023. Control and Data Flow in Security Smell Detection for Infrastructure as Code: Is It Worth the Effort? In *Proceedings of MSR'23: Proceedings of the 20th International Conference on Mining Software Repositories*

VRIJE UNIVERSITEIT BRUSSEL

Software Languages Lab

Research Foundation Flanders
Opening new horizons