Ruby trunk - Misc #14216

webrick: audit and fix Kernel#open misuse

12/21/2017 11:54 AM - normalperson (Eric Wong)

Status:	Closed	
Priority:	Normal	
Assignee:		

Description

Based on Bug #14205 and Bug #14212,
webrick also needs to be checked for Kernel#open misuse.

Associated revisions

Revision edddc28f - 12/22/2017 01:07 AM - normal

webrick: httpauth requires regular files

Be sure we do not try to open a pipe to read from, since we care
about mtime in all cases.

- lib/webrick/httpauth/htdigest.rb: use File.open
- lib/webrick/httpauth/htgroup.rb: ditto
- lib/webrick/httpauth/htpasswd.rb: ditto [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61397 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61397 - 12/22/2017 01:07 AM - normalperson (Eric Wong)

webrick: httpauth requires regular files

Be sure we do not try to open a pipe to read from, since we care
about mtime in all cases.

- lib/webrick/httpauth/htdigest.rb: use File.open
- lib/webrick/httpauth/htgroup.rb: ditto
- lib/webrick/httpauth/htpasswd.rb: ditto [Misc #14216]

Revision 61397 - 12/22/2017 01:07 AM - normal

webrick: httpauth requires regular files

Be sure we do not try to open a pipe to read from, since we care
about mtime in all cases.

- lib/webrick/httpauth/htdigest.rb: use File.open
- lib/webrick/httpauth/htgroup.rb: ditto
- lib/webrick/httpauth/htpasswd.rb: ditto [Misc #14216]

Revision 61397 - 12/22/2017 01:07 AM - normal

webrick: httpauth requires regular files

Be sure we do not try to open a pipe to read from, since we care
about mtime in all cases.

- lib/webrick/httpauth/htdigest.rb: use File.open
- lib/webrick/httpauth/htgroup.rb: ditto
- lib/webrick/httpauth/htpasswd.rb: ditto [Misc #14216]

Revision 646b83af - 12/22/2017 01:07 AM - normal

webrick/httpservlet/cgi_runner.rb: remove unnecessary open

IO#reopen already takes string path names as well as IO objects
(but not "| command" strings)

This makes further auditing for inadvertant code execution
easier. There's no actual bugfix or behavior change here,
as no external data is passed to cgi_runner.rb.

- lib/webrick/httpservlet/cgi_runner.rb: remove Kernel#open call [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61398 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61398 - 12/22/2017 01:07 AM - normalperson (Eric Wong)

webrick/httpservlet/cgi_runner.rb: remove unnecessary open

IO#reopen already takes string path names as well as IO objects
(but not "| command" strings)

This makes further auditing for inadvertant code execution
easier. There's no actual bugfix or behavior change here,
as no external data is passed to cgi_runner.rb.

- lib/webrick/httpservlet/cgi_runner.rb: remove Kernel#open call [Misc #14216]

Revision 61398 - 12/22/2017 01:07 AM - normal

webrick/httpservlet/cgi_runner.rb: remove unnecessary open

IO#reopen already takes string path names as well as IO objects
(but not "| command" strings)

This makes further auditing for inadvertant code execution
easier. There's no actual bugfix or behavior change here,
as no external data is passed to cgi_runner.rb.

- lib/webrick/httpservlet/cgi_runner.rb: remove Kernel#open call [Misc #14216]

Revision 61398 - 12/22/2017 01:07 AM - normal

webrick/httpservlet/cgi_runner.rb: remove unnecessary open

IO#reopen already takes string path names as well as IO objects
(but not "| command" strings)

This makes further auditing for inadvertant code execution
easier. There's no actual bugfix or behavior change here,
as no external data is passed to cgi_runner.rb.

- lib/webrick/httpservlet/cgi_runner.rb: remove Kernel#open call [Misc #14216]

Revision 1895a488 - 12/22/2017 01:07 AM - normal

webrick: add test for WEBrick::HTTPServlet::ERBHandler

This previously had no coverage.

- test/webrick/test_filehandler.rb (test_erbhandler): new test
- test/webrick/webrick.rhtml: new file for test [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61399 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61399 - 12/22/2017 01:07 AM - normalperson (Eric Wong)

webrick: add test for WEBrick::HTTPServlet::ERBHandler

This previously had no coverage.

- test/webrick/test_filehandler.rb (test_erbhandler): new test
- test/webrick/webrick.rhtml: new file for test [Misc #14216]

Revision 61399 - 12/22/2017 01:07 AM - normal

webrick: add test for WEBrick::HTTPServlet::ERBHandler

This previously had no coverage.

- test/webrick/test_filehandler.rb (test_erbhandler): new test
- test/webrick/webrick.rhtml: new file for test [Misc #14216]

Revision 61399 - 12/22/2017 01:07 AM - normal

webrick: add test for WEBrick::HTTPServlet::ERBHandler

This previously had no coverage.

- test/webrick/test_filehandler.rb (test_erbhandler): new test
- test/webrick/webrick.rhtml: new file for test [Misc #14216]

Revision 1989371d - 12/22/2017 01:07 AM - normal

webrick: WEBrick::Log requires path arg when given string

Allowing a user to specify "| command" via Kernel#open is
nonsensical since we never read from the resultant IO.

- lib/webrick/log.rb (initialize): replace Kernel#open with File.open [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61400 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61400 - 12/22/2017 01:07 AM - normalperson (Eric Wong)

webrick: WEBrick::Log requires path arg when given string

Allowing a user to specify "| command" via Kernel#open is
nonsensical since we never read from the resultant IO.

- lib/webrick/log.rb (initialize): replace Kernel#open with File.open [Misc #14216]

Revision 61400 - 12/22/2017 01:07 AM - normal

webrick: WEBrick::Log requires path arg when given string

Allowing a user to specify "| command" via Kernel#open is
nonsensical since we never read from the resultant IO.

- lib/webrick/log.rb (initialize): replace Kernel#open with File.open [Misc #14216]

Revision 61400 - 12/22/2017 01:07 AM - normal

webrick: WEBrick::Log requires path arg when given string

Allowing a user to specify "| command" via Kernel#open is
nonsensical since we never read from the resultant IO.

- lib/webrick/log.rb (initialize): replace Kernel#open with File.open [Misc #14216]

Revision 1ad355bd - 12/22/2017 01:08 AM - normal

webrick/httpservlet/*handler: use File.open

This makes future code audits easier. None of these changes
fix realistic remote code execution vulnerabilities because
we stat(2) before attempting Kernel#open.

- lib/webrick/httpservlet/erbhandler.rb (do_GET): use File.open
- lib/webrick/httpservlet/filehandler.rb (do_GET): use File.open (make_partial_content): ditto [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61401 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61401 - 12/22/2017 01:08 AM - normalperson (Eric Wong)

webrick/httpservlet/*handler: use File.open

This makes future code audits easier. None of these changes
fix realistic remote code execution vulnerabilities because
we stat(2) before attempting Kernel#open.

- lib/webrick/httpservlet/erbhandler.rb (do_GET): use File.open
- lib/webrick/httpservlet/filehandler.rb (do_GET): use File.open (make_partial_content): ditto [Misc #14216]

Revision 61401 - 12/22/2017 01:08 AM - normal

webrick/httpservlet/*handler: use File.open

This makes future code audits easier. None of these changes
fix realistic remote code execution vulnerabilities because
we stat(2) before attempting Kernel#open.

- lib/webrick/httpservlet/erbhandler.rb (do_GET): use File.open
- lib/webrick/httpservlet/filehandler.rb (do_GET): use File.open (make_partial_content): ditto [Misc #14216]

Revision 61401 - 12/22/2017 01:08 AM - normal

webrick/httpservlet/*handler: use File.open

This makes future code audits easier. None of these changes
fix realistic remote code execution vulnerabilities because
we stat(2) before attempting Kernel#open.

- lib/webrick/httpservlet/erbhandler.rb (do_GET): use File.open
- lib/webrick/httpservlet/filehandler.rb (do_GET): use File.open (make_partial_content): ditto [Misc #14216]

Revision f2aa7f40 - 12/22/2017 01:08 AM - normal

webrick/httputils: note Kernel#open behavior

I don't know who uses the load_mime_types method; but it is
conceivable that a user would want to read the results of a
command instead of reading a regular file to load MIME types.

None of the WEBrick-related code in Ruby or default/bundled gems
seems to rely on this method; but it is likely 3rd-party code does.

- lib/webrick/httputils.rb (load_mime_types): note Kernel#open behavior [Misc #14216]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61402 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61402 - 12/22/2017 01:08 AM - normalperson (Eric Wong)

webrick/httputils: note Kernel#open behavior

I don't know who uses the load_mime_types method; but it is
conceivable that a user would want to read the results of a
command instead of reading a regular file to load MIME types.

None of the WEBrick-related code in Ruby or default/bundled gems
seems to rely on this method; but it is likely 3rd-party code does.

- lib/webrick/httputils.rb (load_mime_types): note Kernel#open behavior [Misc #14216]

Revision 61402 - 12/22/2017 01:08 AM - normal

webrick/httputils: note Kernel#open behavior

I don't know who uses the load_mime_types method; but it is
conceivable that a user would want to read the results of a
command instead of reading a regular file to load MIME types.

None of the WEBrick-related code in Ruby or default/bundled gems
seems to rely on this method; but it is likely 3rd-party code does.

- lib/webrick/httputils.rb (load_mime_types): note Kernel#open behavior [Misc #14216]

Revision 61402 - 12/22/2017 01:08 AM - normal

webrick/httputils: note Kernel#open behavior

I don't know who uses the load_mime_types method; but it is
conceivable that a user would want to read the results of a
command instead of reading a regular file to load MIME types.

None of the WEBrick-related code in Ruby or default/bundled gems
seems to rely on this method; but it is likely 3rd-party code does.

- lib/webrick/httputils.rb (load_mime_types): note Kernel#open behavior [Misc #14216]

Revision 7d10b978 - 12/24/2017 08:38 AM - normal

webrick 1.4.2

This release removes uses of Kernel#open to avoid unintended
behaviors and make future auditing easier. [Misc #14216]

6 changes since 1.4.1:

```
  webrick: httpauth requires regular files
  webrick/httpservlet/cgi_runner.rb: remove unnecessary open
  webrick: WEBrick::Log requires path arg when given string
  webrick/httpservlet/*handler: use File.open
  webrick/httputils: note Kernel#open behavior
  webrick/httpservelet/cgi_runner: avoid IO#reopen on pathname
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@61443 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 61443 - 12/24/2017 08:38 AM - normalperson (Eric Wong)

webrick 1.4.2

This release removes uses of Kernel#open to avoid unintended
behaviors and make future auditing easier. [Misc #14216]

6 changes since 1.4.1:

```
  webrick: httpauth requires regular files
  webrick/httpservlet/cgi_runner.rb: remove unnecessary open
  webrick: WEBrick::Log requires path arg when given string
  webrick/httpservlet/*handler: use File.open
  webrick/httputils: note Kernel#open behavior
  webrick/httpservelet/cgi_runner: avoid IO#reopen on pathname
```

Revision 61443 - 12/24/2017 08:38 AM - normal

webrick 1.4.2

This release removes uses of Kernel#open to avoid unintended
behaviors and make future auditing easier. [Misc #14216]

6 changes since 1.4.1:

```
  webrick: httpauth requires regular files
  webrick/httpservlet/cgi_runner.rb: remove unnecessary open
  webrick: WEBrick::Log requires path arg when given string
  webrick/httpservlet/*handler: use File.open
  webrick/httputils: note Kernel#open behavior
  webrick/httpservelet/cgi_runner: avoid IO#reopen on pathname
```

Revision 61443 - 12/24/2017 08:38 AM - normal

webrick 1.4.2

This release removes uses of Kernel#open to avoid unintended
behaviors and make future auditing easier. [Misc #14216]

6 changes since 1.4.1:

```
  webrick: httpauth requires regular files
  webrick/httpservlet/cgi_runner.rb: remove unnecessary open
  webrick: WEBrick::Log requires path arg when given string
  webrick/httpservlet/*handler: use File.open
  webrick/httputils: note Kernel#open behavior
  webrick/httpservelet/cgi_runner: avoid IO#reopen on pathname
```

History

#1 - 12/21/2017 12:05 PM - normalperson (Eric Wong)

normalperson@yhbt.net wrote:

> https://bugs.ruby-lang.org/issues/14216

I don't think there's actual bugs in webrick because of Kernel#open.

The following series tightens down wrong/nonsensical behavior,
and makes future code auditing easier by favoring File.open
instead of Kernel#open.

The only remaining instance of Kernel#open in webrick is in
load_mime_types of webrick/httputils; where I think "|command"

can be beneficial (if the command is used at all).

https://80x24.org/spew/20171221115507.27500-2-e@80x24.org/raw
https://80x24.org/spew/20171221115507.27500-3-e@80x24.org/raw
https://80x24.org/spew/20171221115507.27500-4-e@80x24.org/raw
https://80x24.org/spew/20171221115507.27500-5-e@80x24.org/raw
https://80x24.org/spew/20171221115507.27500-6-e@80x24.org/raw
https://80x24.org/spew/20171221115507.27500-7-e@80x24.org/raw

#2 - 12/22/2017 01:07 AM - Anonymous

- Status changed from Open to Closed

Applied in changeset trunk|r61397.

---

webrick: httpauth requires regular files

Be sure we do not try to open a pipe to read from, since we care about mtime in all cases.

- lib/webrick/httpauth/htdigest.rb: use File.open
- lib/webrick/httpauth/htgroup.rb: ditto
- lib/webrick/httpauth/htpasswd.rb: ditto [Misc #14216]