

Ruby - Bug #12610

webrick: protect from httpoxy

07/21/2016 09:59 PM - normalperson (Eric Wong)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		Backport: 2.1: REQUIRED, 2.2: DONE, 2.3: DONE
Description See problem documented at https://httpoxy.org/ Sorry my Internet connection is crap and I keep dropping. Hope to commit within 24 hours.		

Associated revisions

Revision dafeebf12d4a930a99e5d3917ba070ebefefd23f - 07/22/2016 04:43 PM - Eric Wong

webrick: filter out HTTP_PROXY for CGIHandler

- lib/webrick/httpservlet/cgihandler.rb (do_GET): delete HTTP_PROXY
- test/webrick/test CGI.rb (test CGI_env): new test
- test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@55731 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision dafeebf1 - 07/22/2016 04:43 PM - Eric Wong

webrick: filter out HTTP_PROXY for CGIHandler

- lib/webrick/httpservlet/cgihandler.rb (do_GET): delete HTTP_PROXY
- test/webrick/test CGI.rb (test CGI_env): new test
- test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@55731 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 1bc8bf27665b6b956d882a71fbdd38f34eb289b1 - 08/01/2016 05:26 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 55731: [Backport #12610]

```
* lib/webrick/httpservlet/cgihandler.rb (do_GET): delete HTTP_PROXY
* test/webrick/test CGI.rb (test CGI_env): new test
* test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@55791 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 1bc8bf27 - 08/01/2016 05:26 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 55731: [Backport #12610]

```
* lib/webrick/httpservlet/cgihandler.rb (do_GET): delete HTTP_PROXY
* test/webrick/test CGI.rb (test CGI_env): new test
* test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_3@55791 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 89594c0370bc85d60cd3a06c901316bdf33f60bf - 08/16/2016 04:41 AM - U.Nakamura

merge revision(s) 55731: [Backport #12610]

```
* lib/webrick/httpserver/cgihandler.rb (do_GET): delete HTTP_PROXY
* test/webrick/test CGI (test CGI env): new test
* test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@55923 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 89594c03 - 08/16/2016 04:41 AM - U.Nakamura

merge revision(s) 55731: [Backport #12610]

```
* lib/webrick/httpserver/cgihandler.rb (do_GET): delete HTTP_PROXY
* test/webrick/test CGI (test CGI env): new test
* test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[ruby-core:76511] [Bug #12610]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@55923 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 07/22/2016 02:03 AM - nagachika (Tomoyuki Chikanaga)

As noted in the article (<https://httpoxy.org/>), Net::HTTP and URI::Generic.find_proxy has mitigation about this vulnerability. The remaining issue was that when external programs was spawned in CGI handlers could be effected by HTTP_PROXY env. Is it right?

I don't have ssh key right now, I can commit it and backport at tonight.

How about the stable package releases?

Unfortunately I'm going to be offline this weekend. I can handle the release work on the next monday's night at the fastest.

#2 - 07/22/2016 02:12 AM - darix (Marcus Rückert)

On 2016-07-22 02:03:14 +0000, nagachika00@gmail.com wrote:

0001-webrick-filter-out-HTTP_PROXY-for-CGIHandler.patch (2.46 KB)

the /dumpenv chunk from the patch looks like left over debug code

--

openSUSE - SUSE Linux is my linux

openSUSE is good for you

www.opensuse.org

#3 - 07/22/2016 04:16 AM - usa (Usaku NAKAMURA)

Marcus Rückert wrote:

the /dumpenv chunk from the patch looks like left over debug code

It's not debug code. It's the test for verification.

#4 - 07/22/2016 04:43 PM - Anonymous

- Status changed from Open to Closed

Applied in changeset r55731.

webrick: filter out HTTP_PROXY for CGIHandler

- lib/webrick/httpserver/cgihandler.rb (do_GET): delete HTTP_PROXY
- test/webrick/test CGI (test CGI env): new test
- test/webrick/webrick.cgi (do_GET): new endpoint to dump env
[\[ruby-core:76511\]](#) [Bug [#12610](#)]

#5 - 07/22/2016 04:51 PM - normalperson (Eric Wong)

Marcus Rueckert darix@opensu.se wrote:

On 2016-07-22 02:03:14 +0000, nagachika00@gmail.com wrote:

0001-webrick-filter-out-HTTP_PROXY-for-CGIHandler.patch (2.46 KB)

the /dumpenv chunk from the patch looks like left over debug code

Nope, it's part of the test case as usa said.

Committed as r55731

#6 - 08/01/2016 05:26 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: REQUIRED to 2.1: REQUIRED, 2.2: REQUIRED, 2.3: DONE

ruby_2_3 r55791 merged revision(s) 55731.

#7 - 08/16/2016 04:41 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.1: REQUIRED, 2.2: REQUIRED, 2.3: DONE to 2.1: REQUIRED, 2.2: DONE, 2.3: DONE

ruby_2_2 r55923 merged revision(s) 55731.

Files

0001-webrick-filter-out-HTTP_PROXY-for-CGIHandler.patch	2.46 KB	07/21/2016	normalperson (Eric Wong)
---	---------	------------	--------------------------