Ruby - Bug #5418

Some properties of WEBrick::HTTPRequest could be malformed

10/07/2011 12:01 PM - nahi (Hiroshi Nakamura)

Status:	Rejected		
Priority:	Normal		
Assignee:	normalperson (Eric Wong)		
Target version:			
ruby -v:	-	**Backport:**	

Description

Original reported issue: CVE-2011-3187

Users may expect that properties of WEBrick::HTTPRequest to be not malformed/faked. But at the fact, in current implementation, following properties can be malformed and faked by HTTP header sent by attacker.

- HTTPRequest#host
- can be malformed/faked by 'x-forwarded-host'
- can be faked by 'Host'
- HTTPRequest#port
- can be faked by 'Host'
- HTTPRequest#server_name
- can be malformed/faked by 'x-forwarded-server'
- HTTPRequest#remote_ip
- can be malformed/faked by 'x-forwarded-for' and 'client-ip'
- HTTPRequest#ssl?
- can be faked by 'Host'
- HTTPRequest#meta_vars (Hash of meta vars such as 'REQUEST_URI')
- can be malformed/faked by some HTTP headers

Here's the list of reason why we're thinking it's not a high-priority security bug at this moment.

- For faked data issue, we don't have a way to guarantee that it's not faked. So developers of HTTPRequest must aware of that.
- For malformed data issue, it should be a bug of HTTPRequest to be fixed, but it's the same problem for x-forwarded-host, x-forwarded-server and client-ip. We're offering those data in as-is basis from HTTP header so we can expect users handle the data properly for their purpose (for dumping to xterm, embedding to HTML, etc.)
- And the fix for this bug would be a little complex for quick-fix because it's not only x-forwarded-for which causes this issue. 'client-ip' needs care, too. Documentation would be enough for server_name. We think we need general development cycle for fixing it.

ref:
https://bugzilla.novell.com/show_bug.cgi?id=673010
http://webservsec.blogspot.com/2011/02/ruby-on-rails-vulnerability.html

History

#1 - 03/18/2012 06:46 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

#2 - 02/17/2013 07:08 PM - ko1 (Koichi Sasada)

- Target version changed from 2.0.0 to 2.1.0

Time up for 2.0.0.

Nahi-san, how about this ticket?

#3 - 01/30/2014 06:16 AM - hsbt (Hiroshi SHIBATA)

- Target version changed from 2.1.0 to 2.2.0

#4 - 01/05/2018 09:00 PM - naruse (Yui NARUSE)

- Target version deleted (2.2.0)

#5 - 08/09/2018 08:56 AM - naruse (Yui NARUSE)

- Assignee changed from nahi (Hiroshi Nakamura) to normalperson (Eric Wong)

As Rails did, webrick seems to need introduce TRUSTED_PROXIES.

#6 - 12/24/2020 10:21 AM - hsbt (Hiroshi SHIBATA)

- Status changed from Assigned to Rejected

WEBrick has been removed from ruby repository.

If anyone interest this, Please file this to https://github.com/ruby/webrick