Backport191 - Bug #1767

cgi/session/pstore generating filenames with to less randomness

07/13/2009 08:29 AM - ckruse (Christian Kruse)

Status:	Assigned
Priority:	Normal
Assignee:	xibbar (Takeyuki FUJIOKA)
Target version:	
ruby -v:	ruby 1.9.1p129 (2009-05-12 revision 23412) [x86_64-linux]

Description

=begin
Hi there,

after looking through the code of cgi/session/pstore.rb of ruby 1.9.1 I noticed how filenames are created. Line 48 ff a md5 digest is generated over the session id and then the first 16 bytes of the hex string representation of the checksum are used as the filename (together with a prefix).

```
48      id = session.session_id
49      require 'digest/md5'
50      md5 = Digest::MD5.hexdigest(id)[0,16]
51      path = dir+"/"+prefix+md5
```

While I undestand that one cannot use a full blown SHA512 hash due to the restrictions of the filename, I really don't understand to do something like that. Since MD5 already is considered weak, the count of possible hashes generated by this method are shortened by 50%. It seems to be pretty clear to me that this makes the algorithm vulnerable to several collision attacks for session hijacking; the attacker doesn't has to get the full MD5 hash, he only has to get the HALF MD5 hash to hijack the session.

With the additional known collisions for the MD5 algorithm itself I think it would be relatively easy to hijack the session just bei intelligent brute force.

Greetings,
CK
=end

History

#1 - 07/19/2009 11:24 PM - xibbar (Takeyuki FUJIOKA)

- Assignee set to xibbar (Takeyuki FUJIOKA)

=begin

=end

#2 - 09/14/2010 04:26 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

=begin

=end