Redmine - Defect #31968

MIME Content Type is not properly handled while attaching the files

2019-08-28 08:19 - Amit Mehendale

Status:	Resolved	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Attachments	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	4.0.4

Description

Recently upgraded to 4.0.4. While doing the Information security testing, Team raised a vulnerability
"The application does not validate the content type of file being uploaded. This would enable an adversary to upload a malicious file onto the server."

If I change the extension of a file from **.com** to **.pdf**, Redmine allows file upload in issues as attachment and stores contenttype as "*application/pdf*" in table.

Due to this issue we are unable to roll out new version.

Urgent help required.
Thanks

History

#1 - 2019-08-28 09:35 - Go MAEDA

- Category changed from Files to Attachments

#2 - 2019-08-28 12:26 - Go MAEDA

What do you think about this workaround? It prevents web browsers from opening crafted PDF files inline.

```
diff --git a/app/models/attachment.rb b/app/models/attachment.rb
index a334024b4..3ec3e0e69 100644
--- a/app/models/attachment.rb
+++ b/app/models/attachment.rb
@@ -249,7 +249,7 @@ class Attachment < ActiveRecord::Base
   end

   def is_pdf?
-    Redmine::MimeType.of(filename) == "application/pdf" 
+    Redmine::MimeType.of(filename) == "application/pdf" && MimeMagic.by_magic(File.open(diskfile)).type == 'application/pdf'
   end

   def is_video?
```

#3 - 2019-08-28 13:01 - Amit Mehendale

Thanks for prompt help.

Made necessary Changes. Still file is getting uploaded in the system.

We need to block the upload itself if both types are not matching.

#4 - 2019-08-28 14:41 - Amit Mehendale

- File attachment.rb added

- Status changed from New to Resolved

added a new code in attachment.rb, en.yml(for custom error message).

Attaching new file for further reference.

Thanks for the help

Files

WinSCP.pdf	286 KB	2019-08-28	Amit Mehendale
attachment.rb	16 KB	2019-08-28	Amit Mehendale